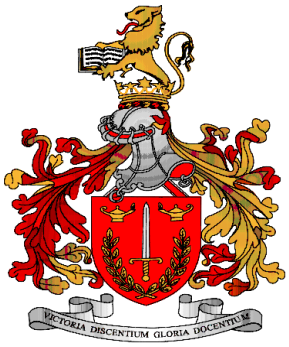
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA



Nélson Tiago Carvalho Silva

Aspirante a Oficial de Polícia

Trabalho de Projeto do Mestrado Integrado em Ciências Policiais

XXIV Curso de Formação de Oficiais de Polícia

CIBERSEGURANÇA

- UM PARADIGMA INTERNACIONAL DE EMINENTE COOPERAÇÃO POLICIAL -

Orientadora:

Professora Doutora Ana Paula Brandão

Lisboa, 26 de abril de 2012

NÉLSON TIAGO CARVALHO SILVA

Aspirante a Oficial de Polícia

CIBERSEGURANÇA

- UM PARADIGMA INTERNACIONAL DE EMINENTE COOPERAÇÃO POLICIAL -

Orientadora:

PROFESSORA DOUTORA ANA PAULA BRANDÃO

Trabalho de final de Curso conducente à obtenção do grau de Mestre em Ciências Policiais e conclusão do XXIV Curso de Formação de Oficiais de Polícia.

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

26 de abril de 2012

DEDICATÓRIA

Às Mulheres da minha vida:

Minha Mãe Maria Dina, exemplo de carinho e ternura;
Minha irmã Alexandra, incondicionalmente presente;
Sobrinhas Marta e Diana, seres mais irritantes que conheço, Amo-vos;
Liliana, minha namorada e futura esposa;

E a meu querido Pai:

Nélson da Silva, dos maiores exemplos com que a vida me presenteou.

AGRADECIMENTOS

Este trabalho simboliza o culminar de cinco anos de trabalho. Desde já tenho que agradecer à minha família, quem mais sentiu a minha ausência nesta etapa da minha vida. No mesmo sentido alargo este agradecimento à minha namorada, que incondicionalmente tem aceitado as minhas escolhas. Porque ainda jaz alguém esquecido por entre as dedicatórias, merece aqui a devida vénia o meu cunhado, Artur, sempre pronto. A todos vós, o mais profundo agradecimento! Na certeza de que sem o vosso apoio incondicional este trabalho não existiria.

Ainda subjacente a estes cinco anos, o XXIV CFOP, a quem tenho a honra de também poder chamar família, merece a gratidão que sempre me acompanhará.

Quanto ao trabalho que segue, apraz-me fazer os devidos agradecimentos. Antes de mais à minha Orientadora, Sr.ª Pr.ª Ana Paula Brandão, que em momento algum poupou esforços na orientação deste trabalho. A si, o mais profundo e sentido Obrigado!

Pessoa marcante neste último ano foi sem dúvida, a nossa Orientadora de Estágio, a quem devemos o merecido agradecimento. Por tudo, obrigado!

Agradeço do mesmo modo a todos os entrevistados, por terem acedido aos nossos pedidos e ânsias. Com especial evidencia o Prof. José Tribolet e Benjamin Silva Rodrigues que marcam certamente a nossa caminhada académica nos trilhos da Cibersegurança. Também a Exma. Srª Eneken Tikk que não olvidou esforços para nos auxiliar. À Exma. Srª Ana Paula Espírito Santo que nos encaminhou nesta nossa pioneira caminhada dos trabalhos científicos.

Por último resta-me agradecer à Polícia de Segurança Pública por me ter acolhido em seu lar.

Não me alongarei mais em agradecimentos, é de facto injusto ter de o fazer pois o espaço não é certamente suficiente para agradecer a todos os envolvidos, quer neste trabalho, quer ao longo destes cinco anos.

"Suae Quisque Fortuna Faber Est"

(O homem é o arquiteto do seu próprio destino)

RESUMO ANALÍTICO

O frenesim que gira em torno da evolução das Tecnologias de Informação e Comunicação levou as atuais sociedades a migrar para o espaço imaterial designado por Ciberespaço. A *internet* catapultou decisivamente, do mundo real para o mundo virtual, uma sociedade global que cada vez mais se afirma digital. Em pleno séc. XXI, onde os Estados vêm a sua autoridade questionada por uma miríade de ameaças transnacionais, surge a Tecnologia que introduz novas variáveis à equação dessas mesmas ameaças. Os crimes tradicionais, inerentes à condição humana, também estes tendem cada vez mais a utilizar as ferramentas que as tecnologias apresentam, migrando desta feita a par e passo com o ser Humano Homem para o Ciberespaço. Perante este quadro, o Estado por si só vê dos seus esforços resultarem incapacidades de travar este fenómeno onde se afirmam as Ciberameaças. A solução afirma-se na cooperação global entre Estados com vista a uma posição comum face ao mais transnacional de todos os crimes, o Cibercrime. Vários organismos Internacionais; como a Organização das Nações Unidas, a União Europeia e o Conselho da Europa; têm enveredado esforços nesse sentido. Cabe às polícias, enquanto monopólio legítimo do uso da força do Estado, prevenir, combater, perseguir e investigar quem colocar em causa o estado de Cibersegurança. A presente dissertação incide sobre o papel da Europol e Interpol, pois estas detêm as ferramentas de cooperação policial entre Estados, na prevenção e o combate da Cibercriminalidade. O primeiro capítulo traça a evolução da sociedade a par da necessidade de governação do Ciberespaço, contemplando a definição e caracterização das Ciberameaças. No segundo capítulo são identificadas as principais ferramentas que têm vindo a ser desenvolvidas pelas Organizações Internacionais em geral, e pela União Europeia em particular. O último capítulo; analisa a atividade da Europol e da Interpol na prevenção e combate à cibercriminalidade, problematizando-se os setores que carecem de cooperação policial. Da investigação surge uma avaliação do contributo destas estruturas cooperativas internacionais para a prevenção e combate da ameaça.

PALAVRAS-CHAVE: Cibersegurança, Cibercriminalidade, Prevenção, Cooperação Policial, União Europeia, Europol e Interpol.

ABSTRACT

The frenzy that involves the evolution of Information and Communication's Technologies led the current society to migrate into the immaterial space so called Cyberspace. The Internet has decisively propeled a global society from real to virtual world, that is increasingly being digital. In the 21st century, where the States have their authority questioned by a myriad of transnational threats, technology adds new variables to the equation of those threats. Traditional crimes, inherent to the human condition, are also increasingly tending to the (mis)use of technology's tools, migrating to the Cyberspace. In this context, States see it their efforts resulting in failure while trying to halt this phenomenon called Cyber Threats. The solution requires global cooperation among States in order to achieve common position against the most transnational of all crimes, Cybercrime. Several International Organizations are aware of this problem implementing measures to deal with it; like United Nations, European Union and Council of Europe. Law Enforcement Agencies, the State´s legitimate monopoly in the use of the force, must prevent, fight, investigate and prosecute those endanger Cybersecurity. This thesis focuses on Europol and Interpol's role, since they hold cooperation mechanisms to prevent and fight against Cybercrime. The first chapter describes the evolution of society along with the need of Cyberspace governance, considering the definition and characterization of cyber threats. The second chapter identifies the main tools that have been developed by International Organizations in general, and by European Union in particular. The last chapter analyzes Europol and Interpol's activity facing Cybercrime, it also questions the sectors that are in need of police cooperation. In sum this dissertation makes an assessment of the contribution of those international cooperative institutions to prevent and fight against Cybercrime.

KEYWORDS: Cyber Security, Cyber Criminality, Prevention, Law Enforcement Agencies' Cooperation, European Union, Europol and Interpol.

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

CC – Convenção sobre o Cibercrime

CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence (Centro de Excelência de Ciberdefesa Cooperativa da NATO)

ComE – Comissão Europeia

CEur – Conselho Europeu

CIA – Central Intelligence Agency

COE – Conselho da Europa

CUE – Conselho da União Europeia

DUDH – Declaração Universal dos Direitos do Homem

EES – Estratégia Europeia de Segurança

EM – Estados Membros

ENISA – European Network and Information Security Agency (Agência Europeia para a Segurança das Redes e da Informação)

EUA – Estados Unidos da América

Europol - Serviço Europeu de Polícia

FBI – Federal Bureau of Investigation

G8 – Grupo dos Oito

ICN – Infraestruturas Críticas Nacionais

II – Instituto de Informática

Interpol - Organização Internacional de Polícia Criminal

ITU – International Telecommunication Union (União Internacional das Telecomunicações)

NATO – Organização do Tratado do Atlântico Norte

NSS – National Security Strategy (Estratégia de Segurança Interna, EUA)

OCDE – Organização para a Cooperação e Desenvolvimento Económico

ONU – Organização das Nações Unidas

PCSD – Política Comum de Segurança e Defesa

PE – Parlamento Europeu

PESC – Política Externa e de Segurança Comum

PJ – Polícia Judiciária

PSP – Polícia de Segurança Pública

TIC – Tecnologia de Informação e Comunicação

UE – União Europeia

UNESCO – United Nations Educational, Scientific and Cultural Organisationa (Organização das Nações Unidas para a Educação, a Ciência e a Cultura)

UNICRI – United Nations Interregional Crime and Justice Research Institute (Instituto de Investigação Inter-regional de Crime e Justiça das Nações Unidas)
UNODC – United Nations Office in Drugs and Crime (Gabinete das Nações Unidas sobre Drogas e Crime).

ÍNDICE

INTRODUÇÃO

ENQUADRAMENTO E JUSTIFICATIVA

A evolução do ser Humano sempre deambulou por entre os progressos técnicos da sua espécie. Evolução tal marcada pelos insurgentes avanços tecnológicos que levaram o ser Humano a afirma-se, hoje, um ser inserido numa sociedade informacional virtual. Ensinamento da História é o facto de inerente à invenção do Homem estarem associados comportamentos desviantes, que originam o tradicional sentimento de repúdio à novidade e culminam numa sociedade que além de "informacional" se caracteriza por ser de "risco".

Facto é que o Crime, também ele se aproveita das vantagens da inovação, acomodando-se nas ferramentas e anonimato associados a este novo espaço. A teoria *Hobbesiana* de que o "Homem é o lobo do Homem" (Thomas Hobbes na sua obra "Leviatã", 1651) foi transferida e encontra-se imortalizada no Ciberespaço, tornando-o um espaço passível a ilícitos criminais de várias ordens que ousamos apelidar de "os mais transnacionais de todos". Assim, o Estado enfrenta esta nova realidade das ameaças transnacionais, confronto esse iníquo caso o Estado considere sequer a hipótese de as combater isoladamente.

A "evolução vertiginosa das novas tecnologias da informação e a sua utilização para fins criminosos" tornou-se "um sério problema" (Rodrigues 2009, 606). Problema que cada vez mais os *media* divulgam e que cada vez mais perturbam o quotidiano dos cidadãos. Os Cibercrimes são os "crimes que, hoje, convivem connosco, dormem ao nosso lado, cruzam-se na rua por nós, e que nos provocam elevados prejuízos" (Valente 2004, 304).

Assim as repercussões dos avanços tecnológicos também se sentem na atividade do Estado e da Polícia. Idos são os tempos onde a segurança era garantida pelos *Vigiles* (César Augusto, ano 6 D.C.) onde o cacete, a chibata e o pequeno gládio imperavam ser as ferramentas. Os tempos de hoje almejam "super-polícias informático-digitais" (Rodrigues 2012, 4). E sendo que a cada dia "o Homem reinventa a cidade, enquanto a Polícia guarda a ordem urbana estabelecida, de modo a prevenir a ocupação do espaço público pela delinquência predatória" (Clemente e Fernando 2007, 38). Neste espaço, que é outro, a "Ciberdelinquência predatória" terá de se subjugar à ação do Estado e das Polícias, que se profetiza de bases cooperativas.

Motivos inerentes à escolha do tema são o impacto demasiado danoso do fenómeno para a nossa sociedade, a natureza eminentemente policial que os mesmos abarcam e a atualidade exímia que enceta. A formação nestas matérias, e relativamente à Polícia, configura para nós elevada importância, sendo que o facto do parco trato policial relativamente às mesmas também funcionou como fator de motivação.

PROBLEMÁTICA E HIPÓTESE

A natureza do Ciberespaço; um espaço virtual, não físico ou territorial e intemporal; amplia o caráter transfronteiriço das Ciberameaças, pelo que o controlo da Polícia surge associado a esforços heroicos. Sendo que as próprias ameaças prosperam em qualquer canto do globo, afetando em tempo real a comunidade mundial, torna-se imperativa a cooperação Interestadual e Interpolicial. A cooperação com vista à criação de um espaço europeu de liberdade, segurança e justiça comum é o caminho a seguir nos trilhos do séc. XXI. A União Europeia (UE) tem-se configurando gradualmente como um ator de segurança, que promove, entre outras funções de governação securitária, a proteção do cidadão. Por seu lado, a Europol, Agência da União, e a Interpol, Organização Internacional de vocação universal, consignam a mesma missão relativamente às Polícias dos vários Estados-Membros (EM). Este trabalho incidirá sobre a cooperação policial, que associa as autoridades policiais competentes dos EM da UE, nos domínios da prevenção e deteção de infrações penais e das investigações das mesmas no domínio do Cibercrime, no período temporal entre 2008 e 2011.

O problema central de investigação que formulamos é o seguinte: *As estruturas e os instrumentos de cooperação policial internacional promovem uma coordenação interpolicial eficaz na prevenção e no combate ao Cibercrime?*

Da anterior pergunta de investigação central decorrem duas perguntas de investigação secundárias no âmbito da Cibersegurança:

1 – *Quais os instrumentos utilizados pela Europol e pela Interpol facilitadores da cooperação internacional?*

2 – *Quais os obstáculos à cooperação policial promovida pela Europol e pela Interpol?*

O problema de investigação cingir-se-á Europol e Interpol enquanto estruturas internacionais de cooperação policial. Ainda com vista à resolução do nosso problema de investigação levantamos a seguinte hipótese central:

Existe um défice de coordenação interpolicial, principalmente a nível dos pontos de contacto, a nível Europeu e Internacional, situação que periga o combate e a prevenção eficazes da Cibercriminalidade.

METODOLOGIA

"As considerações metodológicas definem os elementos que devem ser levados em conta ontologicamente e condicionam a produção do saber acerca das características e das propriedades do sistema internacional e de suas partes" (Jesus 2011, 123). Desta feita, o *design* da presente investigação consubstancia uma abordagem qualitativa. O método qualitativo permitir-nos-á "o exame em profundidade dos casos e a interpretação

de fenômenos significativos histórica e culturalmente ao exigir maior atenção ao detalhe" (Ragin 1994 cit. in Jesus 2011, 123).

A modalidade de pesquisa que utilizaremos será o estudo de caso, a escolha do nosso objeto de estudo correlaciona-se no caso individual da cooperação policial internacional no campo da Cibercriminalidade. Visamos assim a "investigação de um caso específico, bem delimitado, contextualizado em tempo e lugar para que se possa realizar uma busca circunstanciada de informações" (Ventura 2007, 383).

O processo de investigação, baseado no estudo de caso versará a observação, a análise documental e a entrevista. Quanto a esta última é nossa intenção contemplar este estudo com entrevistas qualitativas semiestruturadas. A escolha dos nossos entrevistados versou em geral: entidades do Ministério Público, empresas e profissionais da área da segurança das Tecnologias de Informação e Comunicação (TIC), académicos e profissionais técnicos da área; para deste modo obter um *feedback* exterior acerca da cooperação. Em particular idealizamos a participação da Polícia Judiciária na medida que esta detém os pontos de contato da Europol e Interpol, obtendo desta feita o rigor interior necessário.

A análise documental versará sobre fontes primárias e secundárias, designadamente: documentos oficiais de Organismos Internacionais e do Estado Português, artigos de periódicos científicos, livros e capítulos de livros, alocuções de conferências, seminários e colóquios, monografias, dissertações e relatórios técnicos. A análise dos dados recolhidos será realizada por métodos qualitativos. No que concerne às fontes secundárias, privilegiar-se-á a análise documental. A análise de conteúdo será aplicável às fontes primárias e às entrevistas qualitativas, privilegiando a verificação da frequência de juízos e de avaliações, e a sua respetiva intensidade.

ESTRUTURA DA DISSERTAÇÃO

O presente trabalho comporta três principais capítulos. O primeiro, onde numa primordial fase escortinamos a evolução da sociedade a par da necessidade de governação do Ciberespaço, culmina com o enquadramento conceptual que envolve a definição e caracterização das ameaças.

Seguidamente orientamos esforços no sentido de identificar a realidade atual do Cibercrime contrapondo as principais iniciativas a nível internacional que visam promover a cooperação na prevenção e no combate às mesmas, fazendo-se o devido enfoque à União Europeia.

Por último descortinamos a ação policial, baseada na Europol e Interpol, contrapondo-a com o Cibercrime, analisamos uma posição preventiva face a tal fenómeno e identificamos e analisamos os setores que carecem de cooperação e ação policial. Ainda concertante à estrutura da dissertação, cumpre notar que apesar de não

existir um capítulo ou subcapítulo específico à Convenção sobre o Cibercrime (CC), é recorrente a referência à mesma ao longo do trabalho. Uma nota adicional relativa à amálgama de termos redigidos em Português não consagrados pela nossa literatura: optamos por adaptar a terminologia que o nosso quadro legislativo encerra. Assim, neste sentido aponta a Lei do *Cibercrime* (Lei n.º 109/2009 de 15 de setembro) e a Resolução de Conselho de Ministros nº 12/2012 de 7 de fevereiro de 2012 que designa o Centro Nacional de *Cibersegurança.* Ter-se-á de entender que se tornou comum esta tendência para "Ciberpalavrear" (*vide* neste sentido Cavelty 2007, 21).

I. ENQUADRAMENTO TEÓRICO-CONCEPTUAL

I.1. GOVERNAÇÃO DA SEGURANÇA NO ESPAÇO VIRTUAL

Neste primeiro capítulo retratam-se questões relacionadas com o conceito de segurança. Do mesmo modo seguimos sob a égide de espaços virtuais[1], também estes enigmáticos dada a sua distinta natureza. Analisar-se-á o porquê da securitização deste espaço, os seus utilizadores, o espaço em si e as entidades com idoneidade para garantir a segurança do mesmo.

I.1.1. A MIGRAÇÃO SOCIAL PARA O CIBERESPAÇO

Afigura-se útil começar, desde já, pela evolução, caraterização e balizamento do espaço em questão, espaço esse que moldou e molda a sociedade. Nas últimas décadas tem-se observado um crescimento extraordinário na área das TIC[2], estas últimas que começam a tomar forma nos anos 60. Relembra-se neste momento o seguinte episódio:

> Durante uma entrevista nos anos 50, Albert Einstein declarou que três grandes bombas haviam explodido durante o século XX: a bomba demográfica, a bomba atômica e a bomba das telecomunicações. Aquilo que Einstein chamou de bomba das telecomunicações foi chamado, por meu amigo Roy Ascott (um dos pioneiros e principais teóricos da arte em rede), de "segundo dilúvio", o das informações. (Lévy 1999, 13)

[1] Não obstante dos inúmeros debates em torno deste termo, consideremos primariamente a posição mais anacrónica de Pierre Lévy: "A palavra virtual vem do latim medieval *virtualis*, derivado por sua vez de *virtus*, força, potência. (…) No uso corrente, a palavra virtual é empregada com frequência para significar a pura e simples ausência de existência, a realidade supondo uma efetuação material, uma presença tangível". Continua ainda dizendo que "o virtual não se opõe ao real", "contrariamente ao possível, estático e já constituído, o virtual é como o complexo problemático, o nó de tendências ou de forças que acompanha uma situação, um acontecimento, um objeto ou uma entidade qualquer, e que chama um processo de resolução: a atualização"(1997,15-16). "Por contraposição *ao espaço real* o espaço virtual é não físico e sem massa", itálico nosso, (Rodrigues 2009, 68). Do dicionário da Língua Portuguesa abstrai-se que virtual é algo suscetível de se exercer ou realizar, do mesmo modo é algo potencial, que existe em potência.

[2] TIC: "Tecnologias da informação com realce para as tecnologias envolvidas na comunicação de dados. Em rigor, no conceito de tecnologias da informação já está incluído o aspeto de comunicação; o presente termo serve essencialmente para salientar a enorme importância que as redes de computadores em geral e a *internet* em particular tomaram nos nossos dias." (II 2008)

Ousando atualizar a expressão de Einstein, afirma-mos experimentar em pleno século XXI o impacto da "bomba das tecnologias". A evolução das TIC decorreu e decorre a um ritmo acelerado, sendo que existe um momento marcante nesta evolução. Momento esse ocorre com o aparecimento da *internet*[3], que enquanto pilar basilar das TIC, assume cada vez mais contornos de tecnologia eminentemente social. É no final da década de 1990 que, segundo Castells "o mundo inteiro abraçou a Internet, criando uma verdadeira teia mundial" (2005, 89). Repare-se na descrição do fenómeno *internet* proposta por Barlow que coincide com a sua posição na década de 90: "[A] internet é o evento tecnológico mais importante desde a descoberta do fogo"[4] (2010).

A "evolução tecnológica e a utilização da *internet* contribuíram para a formação de uma grande aldeia global" (Nunes 2010, 481). Neste momento as tecnologias acompanham as exigências do frenesim capitalista. É também nesta altura que nos encontramos perante um novo paradigma tecnológico e social, que nos conduziu à designada Revolução Tecnológica que por sua vez nos moldou numa Sociedade e Era Informacional/Digital[5].

Aparenta existir uma união da biologia e da eletrónica, homem e computador[5]. "As pessoas integraram as tecnologias nas suas vidas, ligando a realidade virtual com a virtualidade real, vivendo em várias formas tecnológicas de comunicação, articulando-as conforme as suas necessidades" (Castells 2005, 23). Observa-se assim uma migração, cada vez mais evidente, da sociedade para um ambiente digital[6], um ambiente presente na quase totalidade do nosso contemporâneo quotidiano. Migração que nos transportou para um espaço abstrato, dissimulado e social onde se realizam diversas transações, espaço este que se tem vindo a designar de Ciberespaço[7].

---

[3] "Etimologicamente, a palavra "*internet*" é composta pelo prefixo "*Inter*" que significa um '*elo de ligação entre dois elementos*' e a expressão '*Net'*, cuja origem (…) pretende traduzir a ideia de '*rede*'. Desta forma, dir-se-ia que se trata de uma '*rede de* redes' informáticas. Trata-se de uma *rede de redes planetária* e em que todas estas redes *se colocam em diálogo*." (Rodrigues 2009, 29). *Internet* é uma "imensa rede de redes que se estende por todo o planeta e praticamente por todos os países; os meios de ligação dos computadores desta rede são variados, compreendendo linhas telefónicas tradicionais, linhas digitais, fibras óticas, comunicação por satélite, etc."(II 2008).

[4] Tradução nossa. No mesmo sentido *Vide* Wellman 2004, 194.

[5] Posição ainda interessante de analisar é a de Tribolet (2011), que demonstra a emergência de uma denominada "Sociedade Biónica", num mundo que se assemelha a uma panela de pressão, onde ocorrem infinitas relações. Aparentando existir uma união da biologia e da eletrónica, homem e computador. Este ponto de vista aborda os recursos ativos de uma organização, "processadores de carbono" que significam metaforicamente pessoas, e os "processadores de silício" em sentido figurado computadores.

[6] Digital, em suma, significa tudo o que é passível de ser criado, armazenado, atualizado e disponibilizado sob uma forma não-física. Digital à semelhança de virtual traduz, mais uma vez, o caráter cada vez mais incorpóreo da vivência societal do séc. XXI. Em rigor traduz-se em dados tratados em sequências de dígitos binários. Entenda-se aqui como sinónimo de virtual.

[7] A palavra "Ciberespaço" surge da união dos termos "cibernética" e "espaço". Esta palavra está fortemente associada ao livro "Neuromancer" de William Gibson em 1984, no entanto vários autores são da opinião que já em 1982, na edição de julho da revista OMNI, no artigo de ficção científica "Burning Chrome" o mesmo já a teria utilizado. No dicionário da Língua Portuguesa figura como sendo o "espaço virtual

O dicionário de termos militares e associados do Departamento de Defesa dos Estados Unidos da América (EUA), caracteriza este espaço como um

> domínio global inserido no ambiente informacional que consiste na rede de interdependências de infraestruturas de tecnologias de informação, incluindo a internet, redes de telecomunicações, sistemas de computadores, e processadores e controladores incorporados[8] (2010, 92).

Seguimos a opinião de Ottis e Lorents, apontando que esta definição realmente não nos parece muito perfaz na medida em que apenas abarca a componente tecnológica negligenciando-se a componente humana (2010, 2). As definições mais usuais traduzem sempre a ideia de uma rede global que liga *hardware*[9], *software*[10] e dados, não podemos contudo olvidar o aspeto humano. O ser humano interage de facto com o espaço em questão, fazendo-o torna-se parte integrante dessa realidade.

Estamos, garantidamente, perante um espaço de comunicação aberto, onde todo o mundo está ligado através dos computadores e respetivas memórias (Lévy 1999, 92). A definição mais completa com a qual nos deparamos é a de Rodrigues que define o Ciberespaço como sendo um:

> espaço ideal[izado] de intercomunicação [inter]subjectiva, onde cada sujeito (individual ou colectivo) aparece como centro autónomo emissor e receptor de mensagens produtivas ou não produtivas, informacionais e comunicacionais, procedendo à sua autodeterminação (afirmação) informacional e comunicacional, de formas estético-existencialmente, relevante e diferenciada, com vista à conquista de uma posição economicamente vantajosa ou à afirmação de uma posição informacional ou comunicacional autónoma, ao nível dos ciclos informacionais e comunicacionais que fluem pelos sistemas e redes informáticas, fora ou dentro do contexto dos serviços, fornecidos no âmbito das redes de comunicação electrónicas publicamente acessíveis (2009, 70).

Deste modo podemos reparar na abrangência que o Ciberespaço assume em pleno séc. XXI, onde a sociedade cada vez mais se torna (virtualmente) em rede, levando ao expoente máximo a expressão inicial proposta por Marshall McLuhan, designada "aldeia global".

Vários autores consideram que a *internet* é a pedra basilar de todas estas relações, tornando-se do mesmo modo um dos maiores pilares do Ciberespaço dado que "constitui desta forma, um meio de excelência para circular todo o género de informação, constituindo um portal de interconectividade entre o 'velho mundo', geográfica e

constituído por informação que circula nas redes de computadores e telecomunicações". A definição e estandardização do termo prevê-se na norma IS0/IEC FCD 27032 ainda em desenvolvimento.

[8] Tradução nossa.

[9] Conjunto dos elementos físicos dos equipamentos informáticos. Componentes físicos de um computador por exemplo: rato, ecrã, circuitos integrados, cabos e placas, etc. Tudo o que é palpável neste ambiente.

[10] Por contraposição ao termo anterior, este termo caracteriza a parte lógica, ou seja, o conjunto de instruções e dados que são processados e permitam o funcionamento do *hardware*. Seguindo o exemplo anterior: programas, aplicações, sistema operativo, etc. Enfim o conjunto dos meios não materiais.

temporalmente definido, onde a realidade é tangível e percecionada, e o 'novo mundo da sociedade da informação'" (Santos *et all* 2009, 1). Este novo espaço, aliado à *internet,* caracteriza-se pela magnificência em termos de oportunidades, o benefício do acesso e partilha de informação, a diluição de fronteiras imposta por um *click*, comunicação, enfim, uma panóplia de benefícios associados às TIC utilizadas em rede. "Por um lado, nesta rede impera a liberdade e a oportunidade, a acessibilidade da informação e a capacidade de estar planetariamente em todo o lado em qualquer momento, e por, a incerteza e a volatilidade, a descentralização da informação e uma nova dimensão existencial – o virtual" (*ibid.*, 2).

I.1.2. A CONTEMPORÂNEA SEGURANÇA DESTE ESPAÇO

Devidamente enquadrados, quanto a este novo espaço de eleição das novas sociedades, reflitamos acerca da segurança do mesmo. O primeiro facto a ter em consideração é que o mundo está de facto a ser transportado para este novo espaço societal, veja-se o relatório acerca das TIC da União Internacional das Telecomunicações (ITU), onde se afigura que uma estimativa de cerca de 1/3 da população mundial se encontra *online*[11] da totalidade de cerca de 7 biliões de habitantes[12] (ITU 2011a,1).

A atual aldeia global caracteriza-se como sendo uma Sociedade de Risco de onde surgem os novos perigos e ameaças (Rodrigues 2009). Este "admirável mundo novo" (*ibid., passim*) é assolado pela tecnologia que, segundo Kranzberg, deve ser encarada como não sendo boa nem má, nem neutra (1985 *apud* Castells, 1996/2005). Contudo é claro que o "benefício que determinados Estados retiram das novas tecnologias é incalculável" (Carrapiço 2005, 175). Assim não podemos olvidar que estamos perante "um fenómeno de duas faces" (Giddens 1995, 5), "uma faca de dois gumes" (Carrapiço 2005, 175). A evolução tecnológica apresenta-nos oportunidades de desenvolvimento e progresso, bem como, retrata uma realidade sombria quando o seu uso se foca em atividades ilícitas.

Na mesma esteira de pensamento diz-nos Paula Espírito Santo que a *internet* continuará "a moldar um padrão, cada vez mais, coerente e imprescindível de comunicação e conhecimento no século XXI, para o melhor e para o pior" (2002, 16). Dos ensinamentos da História podemos ainda retirar que toda a grande invenção humana que consigo acarreta progresso, consigo transporta também comportamentos desviantes e uma nova forma de delinquência, neste caso a criminalidade no Ciberespaço (Dechamp

[11] *Online* significa que está ligado, em linha, em rede, capaz de comunicar. Trata-se de um termo de origem inglesa que se popularizou com o advento da *internet*. Opõe-se a *Off-line*, que por sua vez significa desligado, não conectado, fora de linha.

[12] Adianta-se ainda que 45% dos utilizadores têm uma idade inferior a 25 anos (ITU 2011a,1), o que se salientará quando tecermos qualquer comentário acerca da importância da formação e educação em prol de uma cultura global de Cibersegurança.

2005, 99). Assim, temos a malha social acima referida exposta à faceta negativa das TIC, malha esta em crescimento. O relatório da Europol no âmbito da "European Police Chiefs Convention" vinca o facto de que o "desenvolvimento da *internet* e tecnologias associadas irá, não só, colocar novas ferramentas à disposição de todos os grupos criminosos, mas também irá expor novas vulnerabilidades na nossa sociedade da informação"[13] (2011a, 11). Neste sentido Dechamp deixa claro que este é o tipo de criminalidade do futuro dado que cada vez mais infrações são facilitadas e perpetuadas por tecnologias digitais (2005).

Associado ao Ciberespaço existe um sentimento latente de não responsabilização, este facto, em conjunto com demais, tem levado ao surgimento de novos "riscos" e "perigos" que cada vez mais afetam alguns dos Direitos, Liberdades e Garantias das sociedades modernas (Rodrigues 2009). Cada vez mais surgem todo o género de práticas ilícitas potencializadas pelas TIC. Se a sociedade migrou para esta realidade virtual, à escala mundial, torna-se natural que o crime a acompanhe também. Neste sentido, Venâncio, adianta que as TIC "podem ser utilizadas enquanto instrumentos (muitas vezes mais eficazes quer nos danos causados quer no encobrimento da identidade dos seus autores) para a prática de crimes usuais da realidade corpórea e cujo tipo legal está previsto sem considerar a utilização dos meios tecnológicos como um meio integrador do crime" (2011, 18).

Desta feita, tem-se assistido na última década a movimentações claras por parte de Estados e Organizações Internacionais, onde a ordem de serviços se debruça sobre a segurança no Ciberespaço, até porque, relembra-mos, a "banalização do uso da *internet* forneceu motivação quer para o engenho na promoção da comunicação (…), quer para a prevaricação em moldes virtuais" (Santo 2002, 18), à escala mundial. São inúmeras as facilidades que têm gerado a deslocação da atividade criminosa para o Ciberespaço. Santos, Bessa e Pimentel salientam cinco fatores potenciadores desta realidade:

> a redução do custo dos bens tecnológicos; a redução do custo do acesso à Internet; a expansão rápida da banda larga; o aumento do conhecimento e acesso por parte de possíveis ofensores de técnicas e métodos de ocultação de provas digitais, nomeadamente técnicas de encriptação, a compressão digital, a esteganografia (em nota de rodapé: é arte de esconder informação(…)), entre outros; e o acréscimo da literacia computacional por parte da comunidade global de internautas (2009, 6-7).

Torna-se assim urgente tratar as questões de segurança que assolam os Estados modernos, o cidadão "cada vez mais digital" anseia por uma segurança também esta digital, dadas as inúmeras fragilidades, riscos e perigos que o Ciberespaço também

[13] Tradução nossa.

acarreta; e consequência também do flagelo da criminalidade virtual que se tem vindo a sentir. O espaço acessível ao homem sofreu uma profunda alteração com o aparecimento desta realidade virtual onde se espelham as adversidades que habitam o mundo real.

A "sede de segurança" sempre acompanhou o homem, desde o primeiro agrupamento de pessoas em comunidades até à comunidade virtual que hoje toma forma. A segurança é uma necessidade do ser humano, assumindo na clássica pirâmide de Maslow o 2º lugar das necessidades humanas, logo após as necessidades fisiológicas. Torna-se normal a ansia de segurança do cidadão no espaço para o qual migrou pois os "crimes à escala mundial foram redesenhados para tirarem partido das novas TIC"[14] (Williams 2010, 209).

I.1.3. Atores de Segurança Virtual

A segurança hoje não pode ser contida por muros. As fronteiras físicas já não isolam e pouco significam. "A globalização e a Internet propagam os acontecimentos de forma instantânea a todos os países do mundo" (Silva 2007, 42). Os amargurados ataques terroristas de Nova Iorque e Washington em 2001, Madrid em 2004 e Londres em 2005 têm sublinhado a necessidade de reconstruir sistemas globais de segurança à escala planetária. Idos são os tempos em que abordagens realistas do conceito de segurança eram tidas como traves mestras das orientações políticas Estaduais.

A tradicional perspetiva da segurança baseada maioritariamente na dimensão político-militar e estadual foi dissolvida em abordagens globais e não militares onde a tendência tem vido a ser para o alargamento do conceito. Concordamos que assim seja, e percecionamos o conceito de segurança como passível e de imprescindível atualização. Segundo Brandão "neste mundo em mutação acelerada os factos desnudam teorias e conceitos, mostrando os seus limites heurísticos e prospectivos" (2004, 37). As próprias ameaças, potencializadas pela globalização e pelas TIC, estão em constante mutação, sendo necessária uma reflexão global diária que envolva assuntos de segurança. O espaço virtual e consequente migração social que o mesmo acarreta atualmente, é um espaço que por maioria de razão não pode assumir contornos de desgovernação. As instâncias formais de controlo e regulamentação nacionais e supranacionais são chamadas neste ponto do nosso trabalho à reflexão.

A segurança correspondente à utilização das TIC enquanto meio caracterizador da sociedade "passou a integrar os fins de segurança, liberdade e bem-estar protegidos pelo Estado. De espaço de liberdade alheio ao Estado, a Sociedade da Informação passou a 'território' onde o Estado pretende garantir aos seus cidadãos liberdades de

[14] Tradução nossa.

circulação, segurança nas transacções e respeito pela sua privacidade" (Venâncio 2011, 20). Surge, desta feita, e segundo Balão, o Estado como um dos atores mais interessados na criação de um *status quo* onde as TIC terão de ser prossecutoras do interesse nacional (2010, 37).

Para o Estado moderno a segurança dos domínios virtuais assume relevante importância. "É clássico considerar que a existência do Estado se justifica para atingir três grandes fins últimos: bem-estar, justiça e segurança" (Alves 2010, 41). O Estado enquanto monopólio do exercício legítimo da força carrega consequentemente o garante da segurança enquanto direito de cidadania e bem público. A segurança surge então como função ou tarefa fundamental do Estado, ao qual cada cidadão confia parte da sua liberdade em prol da edificação de um bem individual e supra individual (Valente 2009). Queremos com isto apontar que esta visão clássica também se aplica ao Ciberespaço, palco de excelência na prossecução de Direitos, Liberdades e Garantias. No seguimento, o "Estado, os sistemas e as organizações de segurança têm de adaptar a sua resposta às necessidades de segurança dos cidadãos e do próprio Estado" (Oliveira 2006, 15) que agora emanam de ambientes virtuais. Aliás, a segurança nacional "sempre" se inclinou sobre uma espécie de construção social acerca de questões caracterizadas como ameaças, e acerca de respostas desejáveis a essas questões (Cavelty 2009, 180).

Ainda assim, o Estado não é capaz, por si só, de enfrentar os novos desafios que a globalização acarreta, assim, na governação da segurança virtual são chamados outros atores para complementar a ação Estadual. "Numa sociedade globalizada, a segurança é cada vez mais um bem público que deve ser coproduzido pelo conjunto dos actores sociais" (Oliveira 2006, 15). Partilhamos da opinião de que nenhum ator público ou privado dispõe de todos os conhecimentos e recursos que lhe permitem *per si* resolver determinado problema que se apresente à malha social. O caráter transnacional que envolve o virtual está também patente na segurança do mesmo. A governação da segurança deste espaço terá de incluir forçosamente atores internacionais.

Quando aqui nos referimos à governação, chamamos ao nosso discurso a expressão *governance* e toda a teoria internacional que a envolve. Quanto à governação da segurança (aqui no espaço virtual) Kirchner e Sperling dizem-nos que a governação da segurança, numa versão modificada da definição originária de Webber, pode ser definida da seguinte forma:

> um sistema de regras intencional que envolve a coordenação, gestão e regulação de questões através de: múltiplas e distintas autoridades, intervenções de atores públicos e privados, acordos formais e informais; e propositadamente direcionado para resultados políticos específicos[15] (Kirchner e Sperling 2007, 3).

[15] Tradução nossa.

Paul, numa comunicação ao Primeiro-Ministro Francês, diz o seguinte: "[o] carácter transnacional da rede exige que a reflexão seja levada à escala mundial, graças a uma coordenação dos Estados no seio de instâncias europeias e internacionais"[16] (2000, 42). É nesta altura que chamamos ao debate os demais atores supranacionais nas palavras de Sperling:

> Muitas das ameaças contemporâneas que as grandes potências enfrentam são globais quer na origem quer nas consequências. (...) Esses tipos de ameaças que resistem a soluções nacionais e regionais, surgiram como questões cruciais para o público e as elites dos países do G8 e da China; elas são também motivo de preocupação para outros, incluindo os Estados-Membros da União Europeia e outras potências regionais como a Índia, Indonésia ou Brasil. A proeminência relativa da nova agenda de segurança, bem como a proximidade da tradicional varia através de fronteiras nacionais, em grande parte devido ao sentimento nacional de (in) vulnerabilidade face a essas ameaças e à evolução do Estado para uma identidade tardia ou pós-Vestefaliana[17] (Kirchner e Sperling 2007, 263).

Do complexo e imprevisível ambiente pós-Guerra Fria surge um moldado conceito de segurança, que se num primeiro momento se pendeu acerca da natureza da ameaça, mais tarde debruçou-se acerca dos provedores de segurança. O clássico paradigma realista, acima mencionado, tinha a ameaça claramente identificada e definida, hoje em dia o mesmo não se verifica. "A mutação do ambiente de segurança evidenciou os limites do paradigma e do institucionalismo centrados no Estado" (Brandão 2010b, 9). No período pós-Guerra Fria, a ameaça e os riscos assumem a imprecisão, em grande parte graças à multiplicidade de atores que então se apresentam.

A biosfera tecnológica que envolve o mundo físico em conjunto com a globalização potenciaram as ameaças que agora ascendem à escala planetária. Quando trazemos as TIC associadas ao virtual Ciberespaço essa potencialização transcende a um plano ainda maior. Nesta égide de pensamento afirmamos então que a governação da segurança do mundo virtual é missão de todo o ser humano enquanto membro do Ciberespaço. Amado da Silva diz-nos que a segurança deste mundo é uma "área privilegiada de cooperação", de "natureza transversal a toda a sociedade", porque "ultrapassa as fronteiras nacionais (…) e (…) vai muito para além da defesa nacional, enraizando-se no dia-a-dia das pessoas e das sociedades. Daí nasce a permanente necessidade de uma difusão desta preocupação ('awareness') que tem de constituir um pilar da estratégia de segurança" (2010, 479) que proclamamos ser internacional.

Deste modo são chamados à governação da segurança do Ciberespaço: em primeiro lugar o Estado, no plano nacional, enquanto garante da sua própria soberania e

[16] Tradução nossa.
[17] Tradução nossa.

enquanto garante do bem jurídico "segurança" demandado pelo "*Cibercidadão*"[18]; e em segundo lugar, no plano internacional, os demais países, dado o caráter transfronteiriço do fenómeno da globalização potenciado pelas TIC. Aqui a "governança refere-se à regulação de relações em sistemas complexos que pode ser realizada por uma ampla variedade de instituições e práticas públicas e privadas, estaduais e não estaduais, e nacionais e internacionais"[19] (Williams 2010, 206). O Ciberespaço é um sistema complexo de interações entre tecnologia, organizações e indivíduos, donde resulta que qualquer tentativa de governação passará sempre por esta aproximação dinâmica onde a cooperação assume papel de relevância.

Tem de haver ainda o devido espaço aos vários autores que consideram que a este espaço não é possível qualquer regulamentação[20]. No entanto discordamos de tais posições, não podendo nunca o Ciberespaço configurar um espaço anárquico. A realidade do Ciberespaço e da *internet* pode ser virtual, mas não é menos do que a realidade dos restantes meios convencionais de comunicação como o telefone e a televisão. Por isso mesmo é uma realidade a capacidade da sua regulamentação, que como veremos ao longo do trabalho assume caráter de necessidade. Neste sentido, a regulamentação não é apenas possível, é virtualmente inevitável segundo Robinson (1999, 1). Ainda é determinante a visão de Rodrigues ensinando que a *governance* da *internet*, pilar estruturante do Ciberespaço, "é, sem sombra de dúvidas uma questão técnica, política e ética" [21] (2009, 35).

O próprio Ciberespaço constitui em si fatores motivacionais para a prática de ilicitudes, mais ou menos gravosas em termos de resultados. Desde logo a acessibilidade facilitada a potenciais alvos, as dinâmicas de oportunidade, a disponibilidade de informação maliciosa em rede, a falta de censurabilidade e sentimento de impunidade adjacente, a dificuldade de policiamento do espaço virtual, enfim são demais os fatores que exponenciam as ameaças que decorrem do Ciberespaço.

Assim, e atendendo que o caráter transnacional do Ciberespaço exige um esforço transnacional e supranacional no que respeita à governação e regulamentação do espaço virtual, também a governação da segurança do mesmo espaço envolve a mesma transversalidade no que respeita aos atores. Ousamos desta feita introduzir o termo

[18] "*Cibercidadão*": Expressão que caracteriza o cidadão plenamente incluído na Sociedade da Informação. Queremos sublinhar a migração da sociedade para os novos ambientes virtuais/digitais.

[19] Tradução nossa.

[20] Neste sentido, *vide* Barlow na sua Declaração de Independência do Ciberpaço de 1996 (ver bibliografia).

[21] Para um maior aprofundamento *vide* Rodrigues 2009.

Cibersegurança[22], como sendo o objeto da governação da segurança do espaço virtual, na seguinte passagem:

> Os desafios legais, técnicos e institucionais colocadas pela questão da Cibersegurança são globais e de longo alcance, e só podem ser enfrentados através de uma estratégia coerente, que considere o papel dos diferentes atores e existentes iniciativas, no âmbito de uma cooperação internacional[23] (ITU 2009b, 12).

Terminada esta primeira etapa da nossa caminhada, clamamos desde já à necessidade da cooperação que se avizinha inevitável quando a jornada atravessa ambientes incomensuráveis, transnacionais e globais. Ao longo de toda esta nossa jornada iremos notar que nesta "nova *governance* da segurança, todo o contributo é bem-vindo" (Oliveira 2006, 16). "A democratização em curso parece consentir a conclusão de que, na área da defesa e da segurança com geografias estruturalmente comuns, a segurança colectiva definitivamente superará a segurança soberana" (Moreira 2010, 510).

I.2. Caracterização da Segurança e Ameaças

Afirmado o local de eleição das novas sociedades, e introduzidos os riscos inerentes a essa mesma migração, resta-nos, a tentativa de conceptualização e definição das ameaças, riscos e criminalidade inerentes ao Ciberespaço. Importa neste momento salientar que:

> Existem provas de uma tendência para perpetrar ataques cada vez mais perigosos e recorrentes em larga escala contra sistemas de informação cruciais para os Estados ou para certas funções específicas do sector público ou privado. Esta tendência é acompanhada pelo desenvolvimento de instrumentos cada vez mais sofisticados, que podem ser utilizados pelos criminosos para lançar ciberataques de vários tipos (UE 2010a, 10).

Propomo-nos assim, e devidamente enquadrados, a operacionalizar os conceitos estruturantes do nosso trabalho.

I.2.1. Cibersegurança

Não poderemos olvidar que a definição do conceito Cibersegurança[24] se afirma incongruente dada a natureza virtual que envolve estas matérias. Esta temática (essencialmente política no seu âmago) não está devidamente consensualizada internacionalmente, assim, denotam-se várias terminologias: a NATO usa o termo Ciberdefesa; a UE varia entre segurança da rede e informações, segurança das TIC, segurança da tecnologia da informação, segurança da informação, segurança da rede,

[22] Termo devidamente enquadrado *à posteriori*.
[23] Tradução nossa.
[24] Podemos defini-la como sendo a segurança do e no Ciberespaço. A definição e estandardização do termo prevê-se na norma IS0/IEC FCD 27032 ainda em desenvolvimento.

Cibersegurança, entre outros; e por fim os EUA usam a terminologia Cibersegurança (Tikk *et all*. 2010, 101-102). Manteremos a designação de Cibersegurança dada a aproximação ao nosso espetro legislativo e à tendência global de caracterização desta manifestação de segurança.

Não obstante do acima dito atente-se agora à essência da temática, ou seja, a sua implicação e significado. Ainda assim veja-se a conceção de Cheang[25]:

> A segurança do Ciberespaço, ou Cibersegurança, trata da segurança do Ciberespaço. Esta proporciona orientação para lidar com os problemas decorrentes dos *gaps* entre diferentes domínios da segurança no ambiente do Ciberespaço. Ao mesmo tempo a Cibersegurança fornece uma infraestrutura de colaboração entre as partes interessadas na segurança do Ciberespaço[26] (2009, 9-10).

Aclamamos nesta primeira fase que do próprio conceito de Cibersegurança emerge uma necessidade cooperativa "entre as partes interessadas" que consideramos ser o Estado, em si, o cidadão, e os organismos internacionais. Outra visão interessante é a da ITU, e seu "Grupo de Estudo 17"[27] que chegou à seguinte definição:

> Cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, garantias de segurança, diretrizes, abordagens de gestão do risco, ações, formação, boas práticas, garantias e tecnologias que podem ser usadas para proteger o ambiente e a organização do 'Ciberespaço' e os recursos do utilizador. Os recursos da organização e do utilizador incluem dispositivos de computação conectados, pessoal, infraestruturas, aplicações, serviços, sistemas de telecomunicações, e a totalidade de informação transmitida e/ou armazenada no 'Ciberespaço'. A Cibersegurança esforça-se para assegurar a prossecução e manutenção das propriedades de segurança dos recursos da organização e do utilizador contra riscos de segurança relevantes no 'Ciberespaço'. Os objetivos gerais da segurança compreendem o seguinte: Disponibilidade; Integridade, (…); e Confidencialidade[28] (ITU 2009a, 2).

Em particular a Cibersegurança inclui a adoção de legislação apropriada contra o uso indevido das TIC e contra investidas ilícitas à integridade de infraestruturas críticas nacionais (ICN) (ITU 2009b,12). Este tipo de segurança ganhou especial preocupação e relevância após os acontecimentos do 9/11. Existe uma voz cada vez mais forte que entoa o nome da *internet* como detentora de um lugar junto dos réus no julgamento dos ditos acontecimentos. Fortes evidências têm sugerido que os terroristas usaram a *internet* para planear as operações do 9/11. Os computadores apreendidos no Afeganistão supostamente revelam que a Al-Qaeda recolheu informações sobre os alvos e enviou mensagens encriptadas via *internet* (Thomas 2003). No mesmo sentido Kirchner e

[25] Este autor é coeditor da norma ISO/IEC 27032 - Diretrizes da Cibersegurança.
[26] Tradução nossa.
[27] Tradução nossa de "*Study Group 17*" sigla *SG 17* pertence ao Setor de Estandardização das Telecomunicações (ITU-T) da ITU. Este grupo de estudo tem como responsabilidade os estudos relacionados com a segurança, incluindo a Cibersegurança. Este grupo está ativo desde 2009 e findará o mandato em 2012. A definição consequente é da autoria do grupo e foi publicada através da recomendação n.º X.1205.
[28] Tradução nossa.

Sperling apontam que "a preocupação de proteger o Ciberespaço apenas se evidencia após o 11 de setembro"[29] (2007, 167).

Segundo Fisher (2005) a Cibersegurança diz respeito a três aspetos: as medidas de proteção da tecnologia; o grau de proteção que resulta da aplicação dessas medidas, e o plano do empenho pessoal. Apenas é novidade este último, daqui subtrai-se a pesquisa e análise que visarão aumentar a qualidade (eficiência e eficácia). A Cibersegurança é de caráter global cabendo a todos os atores sociais, estando obrigatoriamente sob a responsabilidade do Estado e das instâncias internacionais. Não nos alongaremos em dissecar as diferentes visões internacionais acerca do que realmente é a Cibersegurança, "simplesmente" pensemos tratar-se da segurança do Ciberespaço, das ameaças e riscos que daí advêm, ou seja, trata-se de criar, manter e desenvolver a segurança de todo Ciberespaço.

"Cibersegurança é uma propriedade do Ciberespaço que trata a capacidade para resistir, responder e recuperar de ameaças intencionais e não intencionais"[30] (Rauscher e Yaschenko 2011, 27).

A Cibersegurança caminhará sempre a par e passo com a superintendência da informação, assim, e porque a informação é o bem mais precioso de qualquer organização é conveniente tratar esta realidade com a seriedade necessária.

I.2.2. CIBERAMEAÇAS

Entramos desta feita no lado mais obscuro deste admirável mundo novo, a sua utilização para fins ilegítimos. É nos novos riscos e ameaças do contexto estratégico pós-vestefaliano do período pós-Guerra Fria que surgem potenciadas as ameaças transnacionais e com elas as agora chamadas Ciberameaças[31]. O desenvolvimento tecnológico e conseguintes TIC tiveram um impacto considerável na perceção e emergência das ameaças.

> As conceções de Ciberameaça são muito amplas e também muito vagas, quer em termos do que é visto como ameaça ou do que está a ser ameaçado. Em teoria, os Ciberataques podem ser perpetrados de várias maneiras por alguém que tenha um computador ligado à Internet, e com fins que variam desde jovens hackers, ao crime organizado, ao ativismo político até à guerra estratégica[32] (Cavelty 2007, 28).

Cavelty adianta que este termo denota uma noção muito vaga que abarca o uso das TIC, quer como alvo, quer como uma arma (*ibid.*, 22). Tradicionalmente as ameaças

[29] Tradução nossa.
[30] Tradução nossa.
[31] Traduzido do Inglês comumente usado "Cyber Threat".
[32] Tradução nossa.

são vistas como uma possibilidade futura (riscos) donde pode advir uma calamidade; ora a antecipação a estes desastres futuros justifica a ação governativa do presente.

Poder-se-á dizer que a Cibersegurança emerge da insurgência das Ciberameaças à tradicional segurança do mundo corpóreo. Regra geral as Ciberameaças são entendidas como qualquer tipo de ameaça que provenha ou seja efetuada através do mundo virtual. Por volta dos anos 80 o *boom* tecnológico que se fez sentir e as claras vulnerabilidades associadas à dependência tecnológica que a sociedade experienciara, começaram a moldar o espetro das ameaças. Estas, associadas à época histórica em que surgem, traduzem o tradicional repúdio pela novidade. Repúdio esse que tomou cada vez mais forma com os ataques informáticos que se foram sentido.

> Neste sentido, as Ciberameaças começaram a ser vistas como uma ameaça aos principais valores da sociedade, bem como ao bem-estar económico e social de nações inteiras. Estabeleceu-se ainda que, devido à infraestrutura tecnológica, os ataques mais prejudiciais poderiam ser realizados de inúmeras maneiras, e potencialmente por qualquer pessoa com acesso a um computador que estivesse ligado à internet, e com os mais variados propósitos, desde a pirataria juvenil, ao crime organizado, ao ativismo político até à guerra estratégica. O novo inimigo não era sequer claramente identificável nem associável a um estado em particular. As ferramentas de pirataria podiam ser facilmente transferidas da internet e constantemente tornarem-se mais sofisticadas e interativas. Com este quadro de ameaças difusas e a com ligação às bases da sociedade (infraestruturas críticas) abriu-se a porta que permitiu transformar cada pequeno incidente num potencial assunto de segurança de máxima urgência[33] (Cavelty 2009, 182).

Assim sendo as Ciberameças podem ser enquadradas em vários campos de ação que analisaremos detalhadamente a seguir. A natureza de anonimidade e o caráter global da ameaça em conjunto com a incerteza e domínio das TIC gerou, na representação de segurança da população um sentimento amplificado, bastas vezes pelos *media,* de desassossego em relação a uma possível Cibercatástrofe[34]. Estas representações da situação de segurança assumem por vezes o caráter de anedótico (*ibid*., *passim*). No entanto, não queremos com esta opinião, olvidar o caráter de perigo inerente e eminente ao uso frenético das TIC. Apenas serve esta passagem para introduzir o tradicional papel dos *media,* nesta temática, que por vezes se afasta da sua natura.

Justificando o antes dito acerca da Ciberameaça, vejam-se por exemplo os dados da Symantec[35], em pleno séc. XXI, apontarem para um aumento de 93% do volume de

[33] Tradução nossa.
[34] Traduzido do Inglês "Cyber-doom" utilizada por Cavelty na obra em questão (2009, *passim*).
[35] Seguindo o exemplo de vários órgãos e estruturas internacionais consideramos o trabalho desta empresa privada bastante fidedigno pelo que o citaremos. *Vide* a título de exemplo: OCDE 2007, NATO 2011, UNODC 2010. A própria UE cita esta fonte *vide* UE 2012. A Symantec está também filiada com a ITU e tem participado nas discussões e políticas de Cibersegurança dos Estados Unidos. Adam Palmer, responsável e consultor de Cibersegurança, na nossa entrevista (Apêndice n.º 7) confirma a existência de demais parcerias

ataques baseados na *internet* (serviço *web*) quando comparados os anos 2009 e 2010 e afigura-se que continuem a aumentar (2011, 21). Segundo Berkowitz e Hahn (2003) estas ameaças são normalmente, e em geral, incluídas pelos especialistas em "quatro modos de ataque": negação[36], fraude, destruição e exploração. Desta feita interliga-se neste momento a ameaça ao ataque, ou seja, passamos da "teorista" ameaça à faceta mais "prática" do ataque, os Ciberataques[37]. Estes últimos, como já vimos podem ser perpetuados com intuitos governamentais, criminais, terroristas, comerciais ou simplesmente por brincadeira, vandalismo ou passatempo.

Os atentados à Cibersegurança consubstanciam na sua génese:

> a) destruição de informação e/ou outros recursos; b) corrupção ou modificação de informação; c) furto, eliminação ou perda de informação e/ou outros recursos; d) divulgação de informação; e e) interrupção de serviços[38] (ITU 2009, 8).

Atente-se que as situações anteriores podem ser classificadas como acidentais ou intencionais, consoante a premeditação da ação. Ainda há autores que falam em Ciberameaças ativas e passivas, consoante alteram ou não modificações na informação do sistema, operações do mesmo, ou próprio estado do sistema.

"As Ciberameaças atuais têm um alcance muito vasto em causas e efeitos"[39] (Hollis 2011, 375) no entanto é tradicional associar-se ao *Clusters* das Ciberameaças a Ciberguerra, o Ciberterrorismo e o Cibercrime, como sendo pedras basilares dos Ciberataques. Ambicionamos aqui completar esse *Cluster*, em pleno crescimento secular, explicitando sucintamente cada um deles.

I.2.2.1. CIBERTERRORISMO

Ciberterrorismo é a junção do terrorismo ao ciberespaço, Pollitt articulou estas duas últimas e chegou ao seguinte:

> O Ciberterrorismo é um ataque premeditado, politicamente motivado contra a informação, sistemas informáticos, programas, e dados; o que resultará em violência contra alvos não combatentes, por organizações subnacionais ou agentes clandestinos[40] (Pollitt 1997).

---

público-privadas entre aquela empresa e os EUA, sabemos que estas parcerias são reais e têm implicações nas jornadas legislativas em relação a assuntos de Cibersegurança, nos EUA esta empresa, e seus estudos, em termos de segurança do Ciberespaço desempenha um papel preponderante. No entanto, dada a natureza do nosso trabalho temos de atentar que estes relatórios estão dotados de uma certa carga "*comercial*" ou de "*partis-pris*", ou seja, podem não oferecer total garantia de independência pelo que trataremos a informação daqui proveniente com a devida prudência.

[36] Mais conhecido por Ataque de Negação de Serviços (ataques DoS) ou Ataque de Negação de Serviços Distribuída (DDoS), esta "visa bloquear ou esgotar os recursos disponíveis de uma máquina impedindo que lhe acedam", *vide* Santos, Bessa e Pimentel 2009, p.169-172.

[37] Traduzido do Inglês comumente usado "Cyber attack".

[38] Tradução nossa.

[39] Tradução nossa.

[40] Tradução nossa.

O Ciberterrorismo é o uso do Ciberespaço para fins terroristas como está definido pelo Direito Nacional ou Internacional (Rauscher e Yaschenko 2011, 27). As intenções terroristas são várias, além das políticas, estão também associadas causas económicas, religiosas, sociais ou ideológicas, estas potenciadas pelo uso das TIC prometem ameaças, intimidações e coações ainda mais violentas junto dos Estados, organizações e cidadãos. Os Ciberterroristas podem consubstanciar novos grupos terroristas que emergem do *boom* tecnológico, contudo, existe também um adaptar dos grupos terroristas já existentes no mundo do crime à nova era da informação.

A *internet* auxilia o crime organizado e os terroristas na prossecução dos seus fins, veja-se por exemplo a crise do Kosovo que se apelidou "*The War of Web*", a guerra do Iraque e o exemplo do 9/11 que já associamos anteriormente ao terrorismo. Santos, Bessa e Pimentel dizem-nos ainda que um terrorista atrás de um teclado pode provocar mais estragos do que um atentado à bomba (2009,87). Mais concretamente temos, por exemplo em 2002, a CIA a localizar grupos terroristas, como a Al-Qaeda e o Hezbollah, e o seu interesse nas TIC, onde se o engenho da arte ainda se não possuía era procurado (CIA 2002). O terrorismo convencional encontrou um verdadeiro cenário bélico na era da informação, onde o anonimato é acentuado e o dano em cadeia e em massa é reforçado.

> Os grupos terroristas estão a usar crescentemente as TIC e a internet para: elaborar planos, angariar e branquear capitais, disseminar propaganda, comunicar de forma segura com os seus membros, partilhar informação e conhecimento com grupos semelhantes, comando e controlo, fazer pesquisa, desenvolvimento, recruta de novos membros, gerar apoio internacional, recolher informações, fazer guerra de informações em nome de nações. Adicionalmente a internet ainda oferece: pouca ou nenhuma regulação, público potencialmente enorme, anonimato na comunicação e rápido fluxo de informações[41] (Dogrul *et all* 2011, 32).

Os grupos terroristas ainda utilizam o Ciberespaço para contatarem entre si, divulgarem informação, planear operações, e espalhar o terror numa ainda maior larga escala. E caso necessitem de saber como construir uma bomba artesanal por exemplo, esta informação consta certamente na *internet*[42]*.*

I.2.2.2. INFRAESTRUTURAS CRÍTICAS

Queremos dar a devida importância ao assunto em epígrafe pelo que reservamos um local próprio para o abordar. As ICN estão geralmente correlacionadas com a anterior Ciberameça, bem como com a Ciberguerra, (o que não inviabiliza per si qualquer outro tipo de ataque por díspar ator social), onde se visam obter lesões sérias. Estes tipos de

[41] Tradução nossa.

[42] Este comentário surge em jeito de epigrama pois existem *online,* e correlacionado com o objeto de estudo sites, *blogs* e fórums virtuais onde se podem encontrar ferramentas e informações acerca de como perpetuar um ataque informático. Contudo, faça-se a experiência no *Youtube* ao pesquisar simplesmente por "bomba caseira".

ataques são perpetuados tendo como alvo as TIC destas ICN e como objetivo fortes convicções de destruição, visando-se portanto efeitos físicos violentos. A Cibersegurança "inclui a adoção de legislação apropriada ao uso indevido das TIC para propósitos criminais ou outros que visem afetar a integridade das ICN"[43] (ITU 2009b, 12). Tradicionalmente as ICN são consideradas pontos vitais a defender, repare-se que se referem a matérias de segurança, sobrevivência, bem-estar e funcionamento de um Estado, seus interesses, organizações e cidadãos. A proteção destas tem em vista ataques, negligência e desastres naturais.

Ganuza, Hernández, e Benavente apontam o setor da energia e das infraestruturas de informação como a base de funcionamento das restantes infraestruturas críticas, sendo estas últimas, e no geral, coincidentes entre países. Na generalidade são ICN as seguintes: sistemas e meios de transportes e comunicações, banca, serviços da administração pública, sistemas policiais e judiciais, saúde, emergência, segurança, abastecimento de água, comida e eletricidade, indústria nuclear, bacteriológica e química, sistemas de defesa militar e proteção civil, aviação, monumentos nacionais (2011, 45).

Assim está também patente que as ICN estão interdependentes umas das outras, ou seja, geram-se "'cascatas de 'interdependências' decorrentes das suas interações e do funcionamento dos seus subsistemas" (Nunes 2010, 485). Este efeito dominó entre ICN tem um impacto imprevisível que usualmente em teoria se avizinham catastróficos[44]. Certamente que a abordagem à Cibersegurança terá obrigatoriamente de passar pela proteção destas estruturas.

I.2.2.3. CRIMINALIDADE ORGANIZADA

Segundo a UNICRI cada vez mais se observa a migração de grupos de criminalidade organizada[45] para o Ciberespaço, transportando consigo as atividades tradicionais e construindo-as em redes criminosas *online.* "Estes grupos planeiam, organizam e cometem todas as formas de crime *online* - desde fraude, roubo e extorsão e abuso de crianças"[46] (UNICRI, 2012). Esta passagem retrata cabalmente o fenómeno de migração social a todos os níveis que como vimos não deixam a criminalidade

[43] Tradução nossa.

[44] Por mais que pareça impensável que dum Ciberataque perpetuado no Ciberespaço possam advir consequências físicas e destrutivas, veja-se o caso do Irão em finais de 2009, inícios de 2010. Cerca de 1000 centrifugadoras da central nuclear de Natanz do Irão foram alvo de um Ciberataque, por intermédio do *Stuxnet 44*, que fez girar as centrifugadoras a uma velocidade superior àquela para que estavam projetadas (Albright, Brannan, e Walrond 2010, passim). Os danos foram exclusivamente materiais mas poderia não ter assim ficado escrita esta página da história mundial. A Symantec tem registo de cerca de 3 mil milhões de ataques de *malwares 44* em 2010 e o Stuxnet destaca-se (Symantec 2011a, 4). Um outro relatório evidência ainda que, em 29 de setembro de 2010, existiam 100 mil hospedeiros *44* infetados no mundo com o *Stuxnet* (*idem* 2011c, 5).

[45] Acerca desta temática e correlacionado com o Cibercrime vide UE de 2010a.

[46] Tradução nossa.

organizada à parte do fenómeno. Criminalidade essa que certamente se poderá começar a chamar de Cibercriminalidade Organizada ou Criminalidade Ciberorganizada.

O crime organizado surge cada vez mais associado à evolução das TIC. Neste sentido Carrapiço afirma que a " enorme capacidade de adaptação do crime organizado permitiu-lhe tirar partido do progresso tecnológico, tendo-se tornado até um dos seus principais beneficiários" (2005, 181). A área de atuação da criminalidade organizada tem-se verificado em vários domínios bastante graves como o tráfico de seres humanos, armas, explosivos, arte, veículos, etc. e, segundo Rodrigues, a própria Cibercriminalidade consubstancia uma criminalidade organizada que se encontra veiculada ao fenómeno da globalização (2009, 265-267). Indubitavelmente a eminência das TIC junto do crime organizado será fator predominantemente a ter em conta aquando do controlo e repressão da mesma.

I.2.2.4. HACTIVISMO

O hactivismo, segundo Cavelty, é o casamento de *hacking*[47] e ativismo (2009, 184). E é precisamente neste ponto que faremos as devidas referências, ainda que sucintamente aos *hackers*[48]. Estes últimos caracterizam-se por serem indivíduos com conhecimentos e capacidades técnicos muito desenvolvidos, numa primeira fase surgem como técnicos que exploram as fragilidades dos sistemas com vista à sua melhoria, no entanto foram assumindo contornos menos lícitos através da intromissão e exploração não autorizadas de sistemas, existindo ainda os que fazem este tipo de atividade meramente como *lobby.* Santos, Bessa e Pimentel explicam que esta última geração, a que emprega a técnica de *hacking* para fins maliciosos, de *hackers* é que é responsável pela atual imagem negativa a eles adjacente (2009, 51). E é nesta geração que surge o *hactivismo*.

Os ativistas tradicionais, associados à política, defendem determinados ideais através da mobilização popular com vista a influenciar as políticas de determinado país ou países. São os ativistas que tradicionalmente conhecemos que variam em termos de objetivos e convicções, alternando entre atuações pacíficas e outras mais violentas. Segundo Denning o ativismo utiliza a *internet* de forma normal e não disruptiva como suporte à causa defendida (2001, 241). É assim um meio poderoso para comunicar, divulgar, planear ações e promover ideias e convicções. Um caso completamente díspar

[47] *Hactivism* diz respeito à utilização de técnicas e programas informáticos específicos com vista a explorar fragilidades das TIC. *vide* Santos *et all* 2009, p. 51-84.

[48] O termo inicialmente foi empregue para caracterizar uma pessoa com grandes facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer o que quiser com um computador (Santos *et all* 2009, 51). Normalmente é uma pessoa que utiliza capacidades de programação e conhecimento técnico para obter acesso não autorizado a sistemas informáticos para finalidades maliciosas e criminosas. Contudo, a comunidade de programação prefere utilizar o termo "*cracker*" para essas pessoas; reservam "*hacker*" para qualquer programador muito respeitado e com grandes capacidades.

é o *hactivismo*, pois conjugam-se técnicas maliciosas na deturpação de sistemas para levar a cabo um ativismo considerado ilícito. Santos, Bessa e Pimentel adiantam que o *hactivismo* socorre-se da técnicas de *hacking* "para aumentar a sua visibilidade e capacidade de intervenção e influência" (2009, 81). Denning acrescenta ainda que as técnicas de *hacking* são usadas contra um alvo da *internet* com intenções disruptivas face às normais operações mas sem causar graves estragos (2009, 241).

Exemplos desta realidade são os grupos hactivistas *LulzSec* e *Anonymous* que ultimamente têm feito vários ataques informáticos a instâncias governamentais e várias entidades e empresas conceituadas de vários países.

Avocam a liberdade de expressão na *internet,* a par do tão badalado caso do *Wikileaks,* com o lema de que não perdoam e não esquecem, encarando a *internet* como coisa séria. Exponenciam o art.º 19 da DUDH, liberdade de opinião e de expressão é a ordem de trabalho destes grupos que consideramos ter uma atitude ilícita. E a par de existirem notícias de terem *hackeado* a própria ONU consideram a existência de um órgão intitulado "Nações Unidas do *Hacking*". É um fenómeno que merece a nossa atenção na prossecução da Cibersegurança.

I.2.2.5. MULTIPLICIDADE DE ILÍCITOS ASSOCIADOS

Neste ponto não queremos extrapolar, nem cingir apenas este nosso trabalho ao escortinar das múltiplas ameaças que extravasam do Ciberespaço. Assim fazemos este ponto de viragem, antes da devida abordagem ao Cibercrime, tratando agora os demais fenómenos que não sendo menos importantes merecem a devida referência.

Consideramos então que as ameaças acima e o Cibercrime, no ponto abaixo, configuram o espetro de ameaças mais usuais e danosas para os Estados Modernos. Muitas vezes é difícil descortinar e enquadrar o ilícito em si em cada um destes subtópicos apresentados, pois consideramos que a maioria das vezes configura um caso de Cibercrime. Assim neste espaço de múltiplos atores, múltiplas ameaças múltiplas novas designações de tipologias criminais surgem os seguintes fenómenos: a Ciberespionagem[49], o Cyberstalking[50], Cyberbullying[51], Cyberlaundering[52] e Cibervandalismo[53].

[49] Espionagem através das novas TIC associada quer ao ramo empresarial quer ao setor estadual.

[50] Este fenómeno assemelha-se às formas tradicionais de importunação e consequente apreensão e medo adjacente. Ocorre no novo ambiente digital sob o prefixo *Cyber,* onde *blogues*, *e-mail's* e afins são o meio mais propício para esta atividade.

[51] Fenómeno do *Bullying* no mundo virtual onde à semelhança do anterior se facilita e potenciam provocações, intimidações, ameaças, importunos e amedrontamentos através do "anonimato" virtual.

[52] Respeita a lavagem de dinheiro *online* num ambiente onde o dinheiro virtual impera.

[53] Adulteração/destruição de conteúdos *online,* configura a tradicional destruição de propriedade alheia desta feita assente no espaço virtual.

A natureza militar do fenómeno Ciberguerra extravasa o domínio policial que este trabalho carreia pelo que não aprofundaremos a temática[54]. Não entraremos também na linguagem mais técnica dos ataques mais usuais deste tipo de ilícitos, se assim fizéssemos o nosso trabalho ter-se-ia de basear somente no escrutínio deste tipo de atividades onde abundam termos como *malwares*, *worm´s* e afins. Estes são alguns dos termos que agora começam a surgir bem como ilícitos que há muito existem. Certamente a nossa escolha fica aquém do panorama atual, contudo serve este ponto para fazer a devida referência à criminalidade de maior ou menor grau de organização com impactos gravosos que atingem o próprio Estado ou o comum cidadão na sua lida diária.

I.2.2.6. CIBERCRIME

Definir o Cibercrime é uma tarefa árdua e não reúne o consenso das comunidades que se debruçam sobre a temática em apreço. O Cibercrime surgiu na sua infância com os programadores adeptos de práticas ilegais de *hacking*, até ao advento dos demais adventos criminais virtuais atuais (Williams 2010, 191-192). Desde logo, qualquer tentativa de definição defronta o caráter espacial e temporal, algo incerto, deste tipo de crimes que os demais crimes "terrestres/reais" não apresentam, dado denotarem certas caraterísticas gerais. As caraterísticas do Cibercrime são díspares comparativamente aos tradicionais tipos criminais. "Existe pouca adesão às restrições espácio-temporais características dos crimes convencionais"[55] (Williams 2010, 192). Assim, torna-se natural o controverso debate acerca do que realmente constitui o Cibercrime. O consenso torna-se ainda mais utópico se pensarmos que todo o mundo teria de estar em harmonia, devido ao caráter amplamente transnacional deste fenómeno que inflama o discurso acerca da jurisdição do discurso legal a nível internacional. Vários órgãos e estruturas internacionais que refletem acerca desta temática não avançam com uma definição exata do fenómeno[56].

A forma mais comum de definir o Cibercrime traduz qualquer atividade na qual os computadores ou redes são ferramentas, alvos ou locais de atividades criminosas (ITU 2009b, 17). Esta conceção, e segundo Venâncio, assemelha-se ao conceito de criminalidade informática usual que levanta as "principais dicotomias que dificultam a consagração de um conceito uniforme" (2011,16). Consideramos que o termo "criminalidade informática" corresponde à Cibercriminalidade e consequentemente o

[54] Para um maior aprofundamento vide Libicki 1995; Morris1995 apud Nunes 2010, 488; ITU 2009b, 58-59; Rauscher e Yaschenko 2011, 30 e Hutchinson 2006. A salutar e referênciar os inúmeros e exímios trabalhos perpetuados pela Academia Militar em várias obras da autoria daqueles. Ainda interessante ver a posição do CCDCOE da NATO, *vide* apêndice 11.

[55] Tradução nossa.

[56] Veja-se que nem a CC do COE adotada em Budapeste em 23 de novembro de 2001 não adianta qualquer definição de Cibercrime, deixando-o ao critério da jurisdição individual.

"crime informático" corresponde ao Cibercrime. Do mesmo modo consideramos que os termos: "crime relacionado com computadores", "crime relacionado com informática", "crime de alta tecnologia", "crime tecnológico", "crime de computação", "crimes informáticos", "crimes virtuais", "crimes digitais", "crimes informático-digitais" se referem a Cibercrime, ao longo da evolução e tratamento da temática em apreço denotam-se várias designações para o que hoje se deve denominar Cibercrime. Trata-se da já referida tendência para "Ciberapalavrear" os novos fenómenos bem como das ténues fronteiras que delimitam cada um dos conceitos separadamente.

A Cibercriminalidade[57] tem sido entendida por grande parte da doutrina, e em sentido amplo, como sendo qualquer infração que de qualquer modo implica o uso de tecnologias informáticas (Rodrigues 2009, 76-77). As óticas de visão que incidem sobre este fenómeno são demasiadas e são bastas as teorias que se debruçam sobre este avaliando a informática/computador/redes como objeto, motivo ou ferramenta do crime. Ou seja quando o computador é afetado pelo ato criminoso, é o alvo da atividade ilícita; quando o computador em si é o ambiente onde o crime é cometido, é o motivo do crime; e por último a situação onde o computador é usado para perpetuar o crime, servindo aqui como simples adereço ao *modus operandi* criminal em relação ao crime.

Não pretendemos divagar neste ponto, por entre a exímia doutrina já produzida, com vista a uma definição exata de Cibercrime, consideremos desta feita, e face à complexidade da questão, que o "Cibercrime é o uso do Ciberespaço para fins criminosos como definido pela lei nacional ou internacional"[58] (Rauscher e Yaschenko 2011, 27). Aliás, esta parece-nos a definição mais correta de Cibercrime pois não se olvida, desta feita, qualquer ilícito relacionado com a Cibercriminalidade. Segundo a ITU o facto de não existir qualquer definição de Cibercrime não precisa de ser importante, desde que o termo não seja utilizado como um termo legal (2009b, 18). Interessa sim é entender o fenómeno e a tipologia associada ao mesmo; isto porque o termo Cibercrime inclui uma grande variedade de crimes.

Teremos por base a CC[59] que distingue quatro categorias específicas de ofensas relacionadas ao termo Cibercrime; são elas:

> 1ª - Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos;
> 2ª - Infrações relacionadas com computadores;
> 3ª - Infrações relacionadas com o conteúdo

[57] Entenda-se toda a criminalidade intentada por qualquer parte integrante do Ciberespaço.
[58] Tradução nossa.
[59] A CC do COE é um trabalho pioneiro, de relevo e de índole internacional sobre o crime no Ciberespaço tendo participado na sua elaboração peritos de todo o mundo (Venâncio 2011, 29-30). Trata-se de um trabalho de referência e conceituado na orla internacional pelos demais parceiros.

4ª - Infrações relacionadas com a violação de direitos de autor e direitos conexos. (Título 1, 2, 3 e 4 respetivamente da Secção 1, Capítulo II da CC).

Esta tipologia, segundo a ITU, não é inteiramente coerente, pois não se baseia num critério único que diferencie as categorias. Adianta ainda que existe uma certa inconsistência que leva à sobreposição de categorias. (2009b, 19). Acreditamos que assim seja pois tomando o Ciberterrorismo como exemplo, as ações deste fenómeno abarcam atos que se enquadram em diversas categorias. Ainda a categoria das "infrações relacionadas com computadores" que se foca no método do ilícito criminal torna-se demasiado ampla face aos ilícitos que a CC apresenta sob a égide desse título[60]. No entanto, as categorias propostas são uma base bastante sedimentada para se estudar o fenómeno.

Na primeira categoria qualquer ataque é dirigido à confidencialidade, integridade e disponibilidade dos sistemas e seus dados. Veja-se o acesso ilegítimo não autorizado e indevido (*Hacking* ou *Cracking* informático), a Ciberespionagem, a interceção ilegal, interferência em dados e interferência no sistema que pode consubstanciar em dano relativamente ao sistema e/ou dados e a sabotagem informática.

A segunda categoria cobre as ofensas que utilizam um computador para serem perpetuadas. São exemplos desta categoria os seguintes ilícitos: falsidade informática, burla informática e nas comunicações, fraude, roubo de identidade, falsificação por computador, e uso indevido de dispositivos.

Na terceira categoria incluem-se os conteúdos considerados ilegais, como a pornografia infantil e erotismo; propaganda do suicídio; descriminação racial, religiosa ou sexual; incitação à violência; solicitação, oferecimento ou incitamento de atividades criminosas; jogo ilegal *online*; injúria e difamação; informação falsa; publicação de documentos confidenciais; venda ilegal de produtos muitas vezes também eles ilegais; fornecimento de informações e instruções de atos ilegais. No entanto estes tipos criminais apresentados terão de ser reorganizados e adaptados ao ordenamento jurídico das partes, os conteúdos/ dados ilegais variarão muitíssimo a par da aproximação cultural e política de cada Estado.

Na quarta categoria incluem-se os crimes relacionados com direitos de autor e direitos conexos. As TIC e *internet* contribuem de forma exponencial e potencializadora deste tipo de ilícitos, desde logo pela disseminação da informação e digitalização de dados. Tratam-se aqui assuntos de partilha de ficheiros ao abrigo de direitos de autor e sem a autorização deste último. A situação das "marcas registadas" também enfrentam grandes desafios neste domínio e por motivos homólogos aos já referidos. A pirataria

[60] Nomeadamente a Falsidade e Burla Informática (art.º 7º e 8º CC).

informática assume um papel predominante neste tipo de ilícitos onde a reprodução ilegítima de dados é a égide de atuação destes[61].

Este tipo de ataques são perpetuados por criminosos especializados no admirável mundo novo das TIC. Assim e com propósitos criminais incorrem nas práticas acima descritas através de subterfúgios informático-criminais que exploram as vulnerabilidades dos sistemas. Não entraremos em especificidades técnicas das ameaças/ataques perpetuados, não olvidando contudo a importância do estudo das mesmas. Citaremos contudo a enumeração dos tipos de Cibercrime proposta por de Williams: negação de serviços[62], ataques de vírus, *hacking* de *sites* e sistemas, fraude *online*, violações da propriedade intelectual e roubo online e violência online (2010, 194-207).

Queremos ainda referir a natureza "imprópria ou impura" dos "crimes informático-digitais" (Rodrigues 2009, *passim*). Um crime tradicional, terreste e habitualmente cometido sem recurso a computadores e redes pode ser perpetuado, e até potencializado, com o uso das TIC. Veja-se por exemplo o caso do crime de difamação e injúria tradicional, "os modernos meios de comunicação (electrónica) vieram introduzir a possibilidade de se atingirem os bens jurídicos da honra e consideração das pessoas humanas de forma 'electrónico-digital', daí se justificar a inserção do tratamento dos crimes de difamação e injúria no contexto da criminalidade informático-digital imprópria" (*ibid.*, 386). Atente-se agora nas seguintes situações que também se enquadram no que estamos a debater: ameaças (*cyberstalking*) e propaganda do suicídio. Estamos perante fenómenos já existentes cujo Ciberespaço aprimorou o modo de atuação criminal. Nas malhas do Ciberespaço encontramos um estudo que nos leva a adiantar que o próprio homicídio poderá consubstanciar um tipo de Cibercrime impuro, revelando que um Ciberataque direcionado a um *pacemaker* pode ser fatal se for utilizada a tecnologia *wireless* para manipular e desligar o aparelho (Halperin *et all* 2008, *passim*). Serve este exemplo para enfatizar o caráter cada vez mais virtual do crime, bem como os efeitos cada vez mais nefastos deste tipo de ataques em crescente evolução.

I.3. Conclusão Capitular

Terminamos desta feita o primeiro passo da nossa caminhada de investigação. Não olvidamos o facto da grande importância que demos a este capítulo, justificada pela complexidade do fenómeno e pela grande perigosidade que em si emerge. É importante portanto conhecer concretamente as ameaças, defini-las e entendê-las. A definição de conceitos correlacionados com todo este ambiente virtual torna-se perentoriamente difícil

[61] A redação destas quatro categorias correspondem em parte à enunciação prevista em ITU 2009b p.18-59, por nós reorganizada e completada segundo Rodrigues 2009, Venâncio 2011 e Santos *et all* 2009.
[62] Ataques DoS ou DDoS.

e ambígua pelo que não queríamos que o leitor seguisse em direção ao destino almejado sem estar devidamente enquadrado perante este "admirável mundo novo".

O crime migrou com o cidadão para ambientes virtuais, a globalização e o desenvolvimento das TIC assumem-se como culpadas deste fenómeno, obrigando os Estados a optar por uma posição. Posição essa que se demanda global.

II. Cooperação Internacional no Combate ao Cibercrime

II.1. A Realidade "Cibercriminal" do Século XXI

É de facto "difícil quantificar o impacto do Cibercrime na sociedade. As perdas financeiras causadas pelo Cibercrime, bem como o número de ofensas, são muito difíceis de estimar"[63] (ITU 2009b, 19).

Desde já pelo ambiente virtual, de difícil monotorização, bem como das cifras negras que acompanham este tipo de Ciberataques. Muitas das vezes as vítimas ou lesados são bancos/entidades financeiras que vêm na publicidade da notícia descrédito e prejuízo ainda superior ao realmente causado pelo ilícito Cibercriminal (Rodrigues 2009, 240). No mesmo sentido aponta a UE, classificando as denúncias deste tipo de crime como "inadequadas", sendo que "alguns crimes não são detectados e em parte porque as vítimas (operadores económicos e empresas) não os denunciam por temerem que a exposição pública das suas vulnerabilidades afecte a sua reputação e as perspectivas comerciais futuras" (UE 2010a, 3).

Rodrigues adianta que "no caso de ataques dirigidos contra pessoas físicas, a 'cifra negra' da criminalidade está interligada com a 'invisibilidade' do crime informático(…). Trata-se de um tipo de criminalidade onde a cifra negra é, efectiva e exepcionalmente alta" (2009, 240). Ainda o mesmo autor, utilizando uma expressão de Figueiredo Dias, diz-nos que neste tipo de ilícitos Cibercriminais as cifras negras atingem uma "magnitude extraordinária e dificilmente ultrapassável por qualquer outro e, de todo, incomparavelmente superiores aos casos de condenações" (*idem*, *ibid.*). Tornando-se assim incerto "até que medida é que o Cibercrime é reportado, não só nos relatórios e estudos, mas também aos agentes da autoridade"[64] (ITU 2009b, 62). Repare-se que a Symantec aponta apenas a estimativa de 21%, em 2011, de Cibercrimes reportados às autoridades, o que corrobora o supracitado.

A nível internacional o próprio conceito de Cibercrime não figura como indicador estatístico junto das instâncias policiais e judiciais, sendo a fronteira entre a criminalidade tradicional e económica e os crimes informáticos demasiado ténue, pelo que os mesmos

[63] Tradução nossa.
[64] Tradução nossa.

podem consubstanciar um crime informático na sua génese e não o serem registados como tal. Enfim, é toda esta panóplia de fatores que nos impede a apresentação de números concretos. Segundo a ITU, as estatísticas que se nos apresentam, relativamente à extensão da Cibercriminalidade, estão abertas à interpretação, não havendo de momento provas suficientes que nos permitam prever as tendências e desenvolvimentos do Cibercrime (2009b, 19). A ONU ainda retrata o fenómeno dotando-o de incerteza quanto à vastidão e impacto do mesmo, fazendo referência à insuficiência e não viabilidade de dados e estatísticas relativas ao Cibercrime (ONU 2010a, 1-2).

Dentro das limitações referidas tentaremos, no entanto, apontar o impacto da Cibercriminalidade. Assim veja-se o relatório da Symantec que aponta um valor superior a aproximadamente 291 milhares de milhões de Euros[65] como sendo o ónus financeiro do Cibercrime em 2011 (Symantec 2011b). O FBI (*apud* ITU 2009b, 61), por seu lado aponta que a economia dos EUA em 2005 teve perdas que ascenderam e ultrapassaram os 50 milhares de milhões de Euros[66]. Tal facto justifica-se dado que o Cibercrime atravessa vários domínios que envolvem elevadas quantias monetárias.

Um estudo deste género e feito à escala mundial está claramente comprometido, contudo acreditamos que as perdas financeiras que o Cibercrime nos apresenta são astronómicas e os valores apresentados, a pecar, será por defeito e não por excesso[67]. Goodman e Brenner dizem-nos, neste sentido, que "os custos financeiros do Cibercrime não são apenas difíceis de estimar, os custos financeiros em si representam menos do que todo o dano que este tipo atividade inflige"[68] (2002, 30). E assim se verifica o levado prejuízo, designadamente os custos diretos de reparação/atualização do *software/hardware*, a perda de acesso ao serviço e a perda de informação.

Relativamente às novas tendências, diariamente são introduzidas no mercado das TIC novidades que traduzem atualizações e/ou novos produtos de uma pertinência sem igual. Atualmente vivemos o advento dos dispositivos móveis (sem fios), muitos deles ligados em rede[69], que cada vez mais fazem parte do quotidiano social e levam ao expoente máximo a interconetividade de "tudo e todos em todo o lado", o que se traduz

[65] Convertido à taxa do dia 2012-03-27 no *site* do Banco de Portugal do valor que consta no documento: 388 biliões de Dólares Americanos (USD).

[66] Convertido à taxa do dia 2012-03-27 no *site* do Banco de Portugal do valor que consta no documento: 67 biliões de Dólares Americanos (USD). Preste-se ainda atenção que este valor figura apenas para os EUA e relata apenas o ano de 2005, desta feita e num ambiente onde as ameaças se proliferam de forma violenta, em sete anos, e relativamente ao globo inteiro, acreditamos que o valor apontado pela Symantec poderá não condizer com a realidade por defeito.

[67] Neste sentido Hamadoun I. Touré, Secretário-Geral da ITU, adiantou o valor de 1 trilião de dólares como sendo o impacto global do Cibercrime (vide Touré 2011).

[68] Tradução nossa.

[69] Por exemplo os telemóveis, *smartphones*, *PDA's*, *tablets*, computadores *notebook's*, dispositivos de armazenamento de dados (discos externos, *pen´s USB*, *CD's*/*DVD's*), *MP3's*, etc.

num fator de preocupação[70]. O anteriormente referido cada vez mais se exponencia ao ponto de frigoríficos, máquinas de lavar e secar a roupa e até mesmo balanças se encontrarem ligadas ao Ciberespaço por *wi-fi*[71] onde, através do virtual, enviam mensagens para os seus utilizadores[72]. Em qualquer local podemos hoje ter acesso (e sem fios) à *internet* ampliando-se desta feita o flanco face ao Cibercrime. Será interessante idealizar a figura de Deus omnipresente, com a mais respeitosa comparação, que hoje se pode observar nas TIC, também elas cada vez mais em toda a parte.

Prova disto é a estimativa, para 2018, que aponta o número de subscrições móveis igual ao número global de cidadãos (OCDE/ITU 2011, 17). A mesma fonte, para 2020, aponta o número de 50 milhares de milhões de dispositivos móveis ligados à *internet* por todo o mundo e o número total de 500 milhares de milhões de dispositivos ligados à rede de um qualquer modo (OCDE 2012b, 7). As TIC estão assim bem presentes na nossa sociedade e o risco que advém deste facto é, do mesmo modo, perentoriamente real[73].

Terá de haver então a referência ao conceito de computação em nuvem[74], munido com múltiplas variáveis que consignam a rede e o perigo em tudo e em todo o lado. Várias empresas relacionadas com a segurança das TIC têm vindo a identificar estes dispositivos como sendo a moda dos ataques hodiernos. Dufkova[75] (2012) identifica esta tendência que aqui acabamos de explicitar na nossa entrevista. As nossas fontes do SIS também seguem esta opinião[76].

Estima-se que mais de um milhão de pessoas por todo o mundo sejam vítimas do Cibercrime todos os dias (UE 2012, 2 e Symantec 2011b, 1). O relatório da Symantec adianta ainda que foram vítimas do Cibercrime 50.000 pessoas por hora, 820 por minuto

[70] Acerca desta questão *vide* a entrevista ao SIS e as questões relacionadas com a Webiquidade e o fenómeno da Convergência e evolução tecnológica. No mesmo sentido veja-se o documento da OCDE 2012b (apêndice n.º2).

[71] O *wi-fi* é um serviço que permite o acesso sem fios à rede em locais públicos, são características deste serviço a mobilidade, flexibilidade e conveniência no acesso à *internet*. À parte de grandes tecnicismos, interessa apreender que *wi-fi*à semelhança do termo *wireless* designam redes de comunicações que recorrem à tecnologia sem fios para transferência de dados.

[72] Acerca desta afirmação veja-se a reportagem da CNN intitulada "When refrigerators tweet and washing machines text" no âmbito do evento "Consumer Electronic Show 2011" em *[http://edition.cnn.com/2011/TECH/innovation/01/07/internet.connected.appliances/index.html]*. Interessante de ver ainda o evento deste ano em *[http://www.cesweb.org/].*

[73] Salientam-se ainda a título de exemplo os dados da *Pingdom* (*vide* Pingdom 2012), uma empresa conceituada de monotorização de sites e servidores da *internet,* que aponta números relativos ao número de contas de *e-mail*, *sites online*, e mesmo dados acerca do n.º de utilizadores (note-se que desta empresa destacam-se clientes como a *IBM*, *Microsoft*, *Secunia*, *Vodafone*, *Siemens*, *Greenpeace* e ONU).

[74] Acerca do fenómeno de Computação em Nuvem (*Cloud Computing*) *vide* ENISA de 2009.

[75] Andrea Dufkova, uma especialista da ENISA em segurança de computadores e resposta a incidentes, cuja entrevista nos foi amavelmente cedida (sob um ponto de vista somente pessoal, não existindo um vínculo formal aqui em relação à ENISA pelo que não será possível extrapolar o aqui mencionado para a agência europeia em questão) (apêndice n.º8).

[76] *Vide* apêndice n.º 2.

e 14 por segundo (Symantec 2011b, 1). De acordo com uma apresentação de Hamadoun I. Touré, Secretário-Geral da ITU, os maiores ataques perpetrados no ano passado[77] foram dirigidos a Estados e empresas conceituadas, sendo que admite a existência de demais ataques graves bem como sibila a vinda de muitos mais (2011, 3).

Permanece assim "parcialmente, desconhecido o alcance da criminalidade informático-digital" (Rodrigues 2009, 240), no entanto, os exemplos que temos demonstram o impacto realmente nefasto e em proporções incomensuráveis. Num mundo onde imperam economias frágeis e ataques em larga escala não há espaço para se negar que a abordagem a nível global se afigura urgente.

II.2. Instituições, Instrumentos e Estruturas Internacionais

Como já afirmamos têm-se notado no plano internacional vários movimentos que nos demonstram que a Cibersegurança tem estado no cerne da ordem de trabalhos dos mais diversos organismos internacionais. A importância versada sobre a Cibersegurança transpõe-se na sua previsão nomeadamente a nível legislativo, político, estratégico nacional e supranacional, imbuída num discurso securitário que não olvida o impacto fenómeno da migração dos ilícitos criminais para o Ciberespaço. Os ataques contra os EUA em 2005, Estónia em 2007, Lituânia e Geórgia em 2008[78], tiveram fortes influências nestas movimentações.

No seguimento, tentaremos fazer a referência às iniciativas internacionais de maior relevância perpetuadas no sentido de diminuir o flagelo das Ciberameaças. O nosso olhar sobre o problema será amplo sendo que versaremos mais cuidados nas iniciativas da UE, espaço económico, político e geográfico donde o presente estudo emerge[79].

II.2.1. ONU

[77] Interessante de consultar é o *site [http://hackmageddon.com/]* que retrata com fidedignidade os maiores Ciberataques anunciados nos media onde figuram também os descritos pelo consequente autor.

[78] Embora estes casos tenham sido cunhados como sendo ciberguerras não existem provas concretas que caraterizem os incidentes como tal, aliás reinam termos, quando nos questionamos acerca da proveniência dos ataques, como "não clara", "nenhuma pista conclusiva", não tendo sido possível rastrear concretamente a proveniência dos ataques (ITU 2009b, 59; Tikk *et all* 2010, 23-74).

[79] Sendo que esta nossa abordagem fica muito aquém da globalidade dos esforços intentados no sentido de um clima global de Cibersegurança salientem-se aindar: Associação de Nações do Sudeste Asiático (ASEAN), Comunidade das Nações (Commonwealth), Cooperação Econômica da Ásia e do Pacífico (APEC), Liga de Estados Árabes, Organização dos Estados Americanos (OAS), União Africana (AU), Organização de Cooperação de Shanghai (SCO) e pelo Conselho de Cooperação do Golfo (GCC), a Rússia também é uma potência meritória de destaque em políticas de Cibersegurança. Para completar a visão global que o nosso trabalho enceta *ab initio*, *vide* Apêndice n.º 11 que consubstancia, e à semelhança do iremos fazer abaixo, uma pequena abordagem à NATO e E.U.A. pela importância acrescida no combate à Cibercriminalidade.

A ONU é uma organização de vocação universal que tem por objetivo primordial "a paz e a segurança internacionais", segundo o nº1 do art.º 1º da Carta da ONU (ONU 2001a, 5) unindo sinergias entre os seus atuais EM.

As Nações Unidas preocupam-se com a temática em apreço desde o 8º Congresso sobre a prevenção do Crime e o Tratamento dos Delinquentes, realizado em Havana, Cuba, que data de 1990; onde a Assembleia-Geral adotou uma resolução relativa a legislação inerente a crimes relacionados com computadores. Quatro anos mais tarde foi publicado um manual de cariz essencialmente técnico em matéria de prevenção e perseguição da criminalidade informática[80]. Assim, desde "os inícios da década de 90 a criminalidade informática tem estado sempre presente no centro das preocupações deste organismo internacional" (Rodrigues 2009, 130).

A destacar a Resolução A/RES/55/63[81], adotada em 2000 pela Assembleia Geral relativa ao combate do uso indevido das TIC "que mostra grande número de semelhanças com o 'Ten-Point Action Plan' do grupo G8"[82] (ITU 2009b, 92) e vinca sobretudo a prevenção. Em 2002 a Assembleia-Geral adotou outra resolução relativa à existência de demais abordagens internacionais atinentes ao combate do Cibercrime e soluções de referência existentes[83]. Em 2004 foi criado um grupo de trabalho[84] para lidar com tópicos criminais relacionados com a *internet* onde se enfatiza o interesse da ONU em participar nas discussões internacionais sob esta temática. É ainda, em 2005, no 11º Congresso de Prevenção do Crime e Justiça Criminal em Bangkok, que foi adotada uma declaração que enfatizou a necessidade de harmonização da luta contra o Cibercrime na orla internacional. Por fim, em 2010, no 12º Congresso realizado em Salvador da Baia, teve uma orientação relevante no que respeita ao Cibercrime. Importante salientar que a Declaração de Salvador recomenda à UNODC que forneça assistência técnica e treino para os Estados melhorarem a legislação nacional e formarem autoridades nacionais capazes de fazer face ao Cibercrime. Foi também neste congresso que se debateu e se colocou a hipótese de se estender e aplicar a CC a esta Organização Internacional (ONU 2010b, *passim*).

Ainda terá de haver espaço à devida referência nomeadamente ao trabalho da ITU, a agência especializada da ONU que mais de debruça sobre o Ciberespaço. O que

[80] "Manual sobre a Prevenção e Controlo da Criminalidade Informática".
[81] *Vide* ONU 2001b.
[82] Tradução nossa.
[83] Resolução [A/RES/56/121] de 23 janeiro de 2002.
[84] WGIG (Working Group on Internet Governance) criado no seguimento da WSIS (World Summit on the Information Society).

mais se destaca na ITU é a iniciativa ITU-IMPACT[85], considerada como "a primeira aliança global sem fins lucrativos, no mundo, contra as Ciberameaças. A IMPACT[86] junta especialistas de governos, academias e indústria para melhorar as capacidades da comunidade global quando lidam com Ciberameaças"[87] (ITU 2011c, 1). Os departamentos da ONU que mais têm destacado em relação a este fenómeno são a UNICRI, UNODC e a ITU.

II.2.2. G8[88]/G20

Em 1997, o então G7[89], criou uma Subcomissão do Crime de Alta Tecnologia que lidava com a luta contra o Cibercrime. Em dezembro desse mesmo ano, os Ministros da Justiça e dos Assuntos Internos do G8 adotaram dez princípios e um plano de ação assente em dez pontos que foram aprovados no ano seguinte na Cimeira de Birmingham. Em 1997, a Sub-Comissão criou ainda a "24/7 High-Tech Crime Point-of-Contact Network"[90](USA GAO 2010, 11-12). Na última cimeira do G8/G20, em Paris, esta temática foi largamente debatida, a salientar um comunicado final da *G8/G20 Youth Summit* onde se "reconhece que cada estado membro deve ter legislação nacional adequada a ajudar a enfrentar os desafios do Ciberespaço", no entanto "qualquer abordagem puramente nacional não será suficiente"[91] (G8/G20 2011, 5-7). Esta temática é assumida como prioridade dos Estados envolvidos e apela-se à "extensão, e evolução contínua, da Convenção de Budapeste a todos os estados do G20 e, eventualmente, à totalidade da comunidade global"[92] (*ibid.*, 10).

II.2.3. OCDE

A OCDE caracteriza-se por defender os princípios da democracia representativa e da economia livre de mercado promovendo políticas que melhorem o bem-estar económico e social a nível global. Os esforços relativos a esta temática por parte da OCDE remontam a 1983 quando esta designou, em Paris, um Comité de Especialistas para discutir os crimes relacionados com computadores e a necessidade subsequente de alterações nos códigos penais tendo em vista uma possível harmonização legislativa

[85] A sigla IMPACT provém de "International Multilateral Partnership Against Cyber Threats". Esta aliança conta atualmente com 140 nações sendo considerada a maior aliança global em Cibersegurança, segundo informação retirada da primeira página do *site [http://www.impact-alliance.org/home/index.html]* em 12/04/2012.

[86] *Vide* nota anterior.

[87] Tradução nossa.

[88] Grupo composto por: Canadá, França, Alemanha, Itália, Japão, Rússia, Reino Unido e EUA

[89] Grupo composto pelos países da nota anterior à exceção da Rússia que apenas aderiu em 1997.

[90] Rede disponível 24 horas por dia, 7 dias por semana para "garantir assistência em investigações globais de Cibercrime. Esta rede consiste em cerca de 40 países por todo o mundo, e também trabalha em cooperação com a rede 24/7da Interpol. O objetivo é assegurar que os criminosos não tenham paraísos no mundo" (Schjolberg e Ghernaouti-Hélie 2011, 58; trad. nossa).

[91] Tradução nossa.

[92] Tradução nossa.

internacional relativa a esta temática (Schjolberd et Hubbard 2005, 8; ITU 2009b, 102). Três anos mais tarde, publicou um relatório que analisava a legislação de então com propostas para o combate ao Cibercrime[93]. Segundo Rodrigues este organismo internacional foi o primeiro a debruçar-se sobre as questões relacionadas com o crime informático promovendo o encontro de especialistas desde inícios da década de 80 (2009, 125). O trabalho do grupo criado no seio da OCDE [94] é visível e de grande mérito.

II.2.4. CONSELHO DA EUROPA

O Conselho da Europa (COE) visa a criação de um espaço democrático e legal que respeite os direitos fundamentais, contribuindo para a "estabilidade e segurança comum" da Europa que enfrenta novos desafios e ameaças que exigem respostas efetivas e concertadas"[95] (COE 2005).

Partilhamos da opinião de Rodrigues quando afigura o COE[96] como o "organismo internacional que abordou de forma mais exaustiva a matéria da criminalidade informática e os seus impactos na comunidade internacional" (Rodrigues 2009, 126). De facto foi do âmago do COE que emergiram as recomendações que consideramos como as mais marcantes relativamente à temática em apreço. Os trabalhos remontam ao ano de 1976, data de realização de uma conferência sobre crimes económicos, a qual destacou a natureza internacional dos crimes relacionados com computadores (ITU 2009b, 95). O COE criou, em 1989, um Grupo de Peritos em Delitos Informáticos que adotou uma recomendação[97] fruto de quatro anos de trabalhos, que abordava a temática em apreço em torno dos termos: harmonização legislativa, cooperação e prevenção. Foi neste documento que se identificaram doze tipos de modalidades de crimes informáticos que traduziam a lista mínima de ilícitos a criminalizar pelos EM.

De entre várias recomendações e documentos do COE, revela-se de maior impacto o dia 23 de novembro de 2001, data da cerimónia de assinatura da CC ocorrida em Budapeste. Nessa mesma data 30 países foram signatários da Convenção[98].

[93] OCDE. 1986. "Computer-related Criminality: Analysis of Legal Policy in the OECD Area" OECD: Relatório DSTI-ICCP 84.22 de 18 abril de 1986. Bibliografia retirada de ITU 2009b, p.102.

[94] ICCP - Information, Computer and Communications Policy, este grupo cria linhas de orientação em matéria de Ciberseurança bem como outro tipo de obras bastantes conceituadas acerca desta temática e disponíveis *online* no site deste organismo.

[95] Tradução nossa.

[96] Não se confunda Conselho da Europa (COE) com Conselho da União Europeia (CUE) e com Conselho Europeu (CEur).

[97] Recomendação n.º R(89)9, adotada em 13 de setembro de 1989, na Reunião de Ministro e Deputados n.º 428º. A missão de ser feito um esboço, com a colaboração de vários órgãos e estruturas internacionais, de uma Convenção Internacional era parte integrante da missão deste grupo de trabalho. A versão final deste esboço foi apresentada unicamente no momento de aprovação e início da sessão de ratificação.

[98] Incluindo quatro países não-membros do COE, Canada, EUA, Japão e África do Sul que também participaram nas negociações.

Atualmente existem 47 países signatários da CC, das quais 32 foram ratificadas e 15 não, 30 países já adotaram plenamente a CC[99].

> Países como a Argentina, Paquistão, Filipinas, Egito, Botswana e Nigéria já delinearam partes da legislação doméstica de acordo com esta Convenção. Contudo estes países ainda não assinaram a Convenção.(…) A convenção é hoje reconhecida como um instrumento internacional importante na luta contra o Cibercrime e é patrocinada por diferentes organizações internacionais[100] (ITU 2009b, 96).

Convenção que visa essencialmente:

> 1- Harmonizar os elementos das infracções respeitantes ao direito penal material nacional e as disposições conexas em matéria de cibercriminalidade;
> 2- Fornecer ao direito processual penal nacional os poderes necessários à instrução e à perseguição de infrações deste tipo bem como outras infracções cometidas por meio de um sistema informático ou nas situações em que existem provas sob a forma electrónica, e
> 3- A pôr em funcionamento um regime rápido e eficaz de cooperação internacional[101] (COE 2001b).

De referir ainda o Projeto Global sobre o Cibercrime que enceta já a terceira fase entre 1 de janeiro de 2012 e 31 de dezembro de 2013. O projeto está sedimentado sobre mais de 250 atividades (desenvolvidas na fase 1 e 2) desde 2006 e conta com projetos conjuntos entre este e a UE de onde emerge o objetivo primordial de promover uma ampla difusão da CC com vista à harmonização (COE 2012b, 1).

II.3. A União Europeia Como Garante de Cibersegurança

"A União Europeia impõe-se como um desafio teórico e prático, um caso único que tem produzido uma profusão de conceitos, abordagens e teorias (micro, mesa e macro), sendo manifesta a dificuldade da literatura das Relações Internacionais e da Ciência política em acomodar este actor *sui generis*" (Bretherton e Vogler 2007 *apud* Brandão 2010b). Segundo Brandão os elementos de inovação da UE são sinal de mudança num sistema internacional que combina elementos vestefalianos e pós-vestefalianos (*idem, ibid.*).

A devida referência ao Tratado de Maastricht, 1992, permite-nos adiantar a estrutura da UE mantida até à entrada em vigor do tratado de Lisboa. Estrutura essa assente em três pilares: 1º - o pilar das Comunidades Europeias; 2º - o pilar consagrado à Política Externa e de Segurança Comum (PESC); e por último o 3º - o pilar consagrado à cooperação nos domínios da justiça e assuntos internos[102] (Borchardt 2000, 19). É

[99] Dados obtidos *online* no *site* do COE atualizados até 10/04/2012.
[100] Tradução nossa.
[101] Tradução do ponto 16 do documento em apreço proposta por Rodrigues (2009, 609).
[102] Após a entrada em vigor das alterações do Tratado de Amesterdão, o terceiro pilar ficou restrito à cooperação policial e judiciária em matéria penal.

neste Tratado que se plasma o modelo estadual onde se encontra a separação segurança interna e segurança externa, aqui reforçada em pilares.

No campo de ação do segundo pilar, merece ainda destaque a aprovação, em 2003, da Estratégia Europeia de Segurança (EES)[103]. Ainda no cerne do 2ºpilar e no âmbito da PESC, a UE desenvolveu uma Política Europeia de Segurança e Defesa (PESD), agora designada PCSD[104], onde se revela com maior evidência a *security actorness* da UE. Quanto a estas políticas pode-se revelar a oscilante inclinação da EU no que concerne à confiança depositada num "*hard*", "*soft*" *ou* "*smart power*"[105] para fazer face aos atuais desafios de segurança (Kirchner e Sperling 2007). Quanto a este último não nos pronunciaremos, contudo a PESC configurará o *soft power* onde se evoca um "multilateralismo efectivo" (expressão utilizada na EES 2003, 8). O PCSD introduz uma componente de *hard power* onde as possibilidades de ação externa se veem exponenciadas.

Relativamente à temática em apreço, já na EES de 2003 se encontram referências, ainda que indiretas, como sendo no caso da ameaça do terrorismo onde os atores "estão ligados entre si através de redes electrónicas" (CEur 2003). No entanto as Ciberameaças não figuram entre os desafios globais e principais ameaças ali enunciadas, fazendo contudo a já enunciada afirmação de que "nenhum país é capaz de enfrentar totalmente sozinho os complexos problemas que hoje em dia se colocam" (CEur 2003, 1). Em 2008, o documento que atualizou este primeiro já refere explicitamente a Cibersegurança, contemplada nos desafios globais e principais ameaças à UE. No seguimento, também a Estratégia de 2010, sobre a segurança interna da União[106], consigna a Cibercriminalidade como uma ameaça mundial de cariz prioritário.

Não seria correto seguir o nosso caminho sem a devida referência ao Tratado de Lisboa que introduziu algumas mudanças no cerne da UE. Com a entrada em vigor deste tratado a UE, agora dotada de personalidade jurídica, deixa de estar fragmentada em pilares o que cria condições favoráveis a uma maior coerência de políticas, nomeadamente entre as dimensões interna e externa (Brandão 2011, 2). É ainda na esteira do Tratado de Lisboa que o Tratado sobre o Funcionamento da UE, que se identifica, no seu art. 83º, várias ameaças, caracterizando a "criminalidade informática"

[103] Consultar evolução da EES nos documentos CEur 2003, CEur 2008 e CUE 2010a.
[104] Política Comum de Segurança e Defesa.
[105] "*Hard Power"* e "*Soft Power"* são termos utilizados para caracterizar as estratégias políticas no âmbito das Relações Internacionais. O primeiro caracteriza-se por se tratar de uma posição mais coerciva, uma posição onde impera a coação e imposição; por oposição o segundo prevê a ação baseada na persuasão, inclui termos como a diplomacia e negociação, por exemplo. Ainda de salientar o "*Smart Power",* expressão associada a Joseph Nye, este último conjugará as caraterísticas dos dois primeiros resultando numa combinação harmoniosa de coação e persuasão.
[106] *Vide* UE 2010b.

como sendo "criminalidade particularmente grave com dimensão transfronteiriça" de "especial necessidade de as combater, assente em bases comuns" (UE 2010h, 81).

A salientar de novo a visão de Emil Kirchner e James Sterling às quatro funções da União no domínio da segurança: prevenção, *assurance*, proteção e compulsão. No primeiro visa-se a prevenção de conflitos consolidando-se as instituições democráticas e respetiva sociedade, a segunda debruça-se na garantia e consolidação da paz, na terceira observa-se a vertente da segurança interna e por último temos a implementação da PCSD via construção/manutenção/imposição da paz. Cada vez mais se vê uma União facilitadora de ação conjunta que procura reforçar o seu papel de ator autónomo de segurança (2007 *apud* Brandão 2010a, 51).

II.3.1. DIMENSÃO INTERNA

Quanto à dimensão interna, a estratégia de segurança interna hodierna da UE contempla várias referências à Cibercriminalidade. Antes de mais convém assinalar o papel desempenhado por esta Organização Internacional no que concerne à criação de uma sociedade da informação e comunicação global sustentada numa era comum de informação[107].

Veja-se que a "União deverá, pois, promover a adopção de políticas e de legislação que garantam um elevado nível de segurança das redes e permitam reagir mais rapidamente em caso de avaria ou ataque informático" (CEur 2010, 22). Com a entrada em vigor do Tratado de Lisboa e à luz das orientações fornecidas pelo Programa de Estocolmo[108] e respetivo Plano de Ação a UE dispõe atualmente da oportunidade de avançar com novas medidas.

Desta feita começaremos por fazer referência à Estratégia de Segurança Interna da União[109], onde a Cibercriminalidade é identificada como fator que poderá fazer perigar "os valores e a prosperidade das nossas sociedades abertas" (CUE 2010, 7), note-se que também ainda se ressalva o facto de a demais criminalidade e ameaças graves surgirem como beneficiárias da evolução das TIC. A Estratégia de Segurança Interna foi adotada com o intuito de estabelecer diretrizes e princípios de ação futura com vista a prevenir a criminalidade e reforçar a capacidade de resposta oportuna e adequada a catástrofes.

> A Europa constitui um alvo fundamental para a cibercriminalidade devido à sua infra-estrutura avançada no domínio da Internet, ao elevado número de utilizadores, bem como à importância da Internet para o funcionamento das suas economias e sistemas de pagamento. Os cidadãos, as empresas, os governos e

[107] Neste sentido *vide* Benjamim 2009, p.86-96.

[108] O Programa de Estocolmo é o programa da UE nos domínios da justiça e dos assuntos internos. Neste sentido *vide* CEur 2010 e UE 2010f.

[109] Em fevereiro de 2010, durante a Presidência semestral espanhola, o Conselho completou a EES com a adoção da Estratégia de Segurança Interna, aprovada pelo CEur de 25 a 26 de março de 2010.

> as infra-estruturas críticas devem beneficiar de uma protecção reforçada face aos criminosos que tiram partido das tecnologias modernas (UE 2010b, 4).

Ainda relativamente à dimensão interna e à Estratégia de Segurança Interna da União sobressaí ainda uma comunicação da UE onde se identificam cinco etapas de ação que configuram cinco objetivos estratégicos e ações específicas para o período 2011-2014. Dos cinco objetivos referenciados o objetivo n.º3 consigna-se em "reforçar os níveis de segurança para os cidadãos e as empresas no ciberespaço" (UE 2010b, 10). Ainda uma outra comunicação do Conselho da União Europeia (CUE) estabelece como prioridade, no âmbito da luta contra a criminalidade organizada, no período de 2011 a 2013, o seguinte: "intensificar a luta contra a cibercriminalidade e a utilização criminosa da Internet pelos grupos criminosos organizados" (CUE 2011b, 4-5).

No intuito da prossecução de todos estes objetivos está previsto, até 2013, a criação de um "Centro de Cibercriminalidade"[110], que se quer caraterizado como "o ponto nevrálgico do combate europeu à cibercriminalidade" (UE 2010b, 10). A nível nacional dos EM, prevê-se a criação de centros de excelência nacionais e medidas de cooperação entre academias e empresas. Prevê-se ainda a aplicação de normas comuns pelos serviços policiais, Ministério Público e investigadores forenses na investigação e repressão das infrações penais no domínio da Cibercriminalidade.

"Devem ser tomadas diversas medidas para melhorar a prevenção, a detecção e a resposta rápida em caso de ciberataques ou de perturbações no ciberespaço" (UE 2010b, 11) pelo que até finais de 2012 todos os EM e as próprias instituições da UE devem dispor de uma equipa de emergência de resposta no domínio informático que funcione em boas condições (*ibid.*). A cooperação entre estas e entidades policiais é também enfatizada neste ponto em matéria de prevenção e resposta. Está por último prevista a elaboração de planos de contingência nacionais e realizar periodicamente, bem como exercícios nacionais e europeus em matéria de resposta a incidentes e recuperação em caso de catástrofes, em todos estes pontos a ENISA assume papel de apoio, cooperação, orientação e supervisão.

Em 2007, o documento "Rumo a uma política geral de luta contra o cibercrime"[111] define como objetivo "reforçar a luta contra o cibercrime a nível nacional, europeu e internacional" (ComE 2007a, 4). Dois anos mais tarde, e relativamente à proteção das infraestruturas críticas da informação, surge mais um documento designado "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a

[110] À frente esmiuçado no trecho textual dedicado à Europol dada a vontade de instalar este nos serviços da mesma.
[111] *Vide* ComE 2007a.

preparação, a segurança e a resiliência"[112]. O documento de 2011 que visa as "Realizações e próximas etapas: para uma cibersegurança mundial"[113] mantém a mesma linha dos anteriores, fazendo uma análise do já efetuado e perspetivando-se mais uma vez o esforço global necessário. O sistema europeu de alerta e de partilha de informações já previsto nos objetivos estratégicos relativos à segurança interna[114] surge aqui novamente sublinhado e em desenvolvimento até 2013.

Ainda a focar a iniciativa *e-Europa*, lançada em 1999, e que conta já com inúmeros documentos relacionados, visando proporcionar uma era digital à Europa dentro de um ambiente geral de Cibersegurança. Desta iniciativa salienta-se a comunicação intitulada "Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e lutando contra a cibercriminalidade – *eEurope* 2002"[115], onde se destaca o combate em geral à Cibercriminalidade e em particular à pornografia infantil. Acerca deste último ponto é importante salientar a Diretiva 2011/92/UE[116] do Parlamento Europeu e do Conselho "relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil" que configura um bom exemplo da atenção especial que a Comissão dedica à proteção de crianças, especialmente no que se refere à luta contra todas as formas de publicação ilícita de pornografia infantil através de sistemas de informação.

Por último resta a mais importante para o nosso estudo, Decisão Quadro 2005/222/JAI[117] do CUE, de 24 de fevereiro, relativa à harmonização legislativa e consequente cooperação policial e judicial dos seus EM sobre ataques contra os sistemas de informação. Hert, Fuster e Koops (2006, 522-523), que elaboraram um estudo comparativo entre a CC e esta Decisão, concluem que esta decisão tem instrumentos que em muitos aspetos são comparáveis à CC, duplicando-a, adiantando ainda que as previsões da lei criminal não diferem substancialmente e que apesar disto à Decisão subjaz um valor especial acrescentado dado ser mais forte em termos de previsões relativas a conflitos jurisdicionais. É ainda o Programa de Estocolmo que prevê a ratificação, por parte dos EM, "o mais rapidamente possível" da "Convenção de 2001 do Conselho da Europa sobre a Cibercriminalidade, que deverá constituir o quadro jurídico de referência para combater a criminalidade informática a nível mundial" (CEur 2010, 22). Já uma recomendação do Conselho de 25 de junho de 2001 "relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia" que tinha em conta a posição

[112] *Vide* CE 2009.
[113] *Vide* ComE 2000.
[114] *Vide* UE 2010b.
[115] *Vide* ComE 2000.
[116] Que veio substituir a Decisão-Quadro 2004/68/JAI relativa à exploração sexual de crianças.
[117] *Vide* CUE 2005. *Vide* também documento que prevê a revogação da mesma (UE 2010a).

adotada pelo Conselho Europeu (CEur) já em 19 de março de 1998, no sentido de convidar os EM a aderirem à rede de informações do G8 já referida (CUE 2001, 1).

Finalmente de referir a "Agenda Digital para a Europa"[118] que também aborda a Cibersegurança entre os sete pilares de ação prioritários desta agenda sob a seguinte epígrafe "Confiança e Segurança".

II.3.2. DIMENSÃO EXTERNA

"A crescente afirmação da União como actor internacional suscitou a formulação de abordagens explicativas da dimensão externa de um actor singular e complexo" (Brandão 2010b, 11). Na Estratégia de Segurança Interna da UE reconhece-se a "interdependência entre segurança interna e segurança externa" sendo que a abordagem prosseguida é a de uma "segurança global com os países terceiros" adaptando-se as "necessidades dos cidadãos" com os "desafios" e "dinâmica global do século XXI" (CUE 2010, 8).

No âmbito da já referida comunicação n.º 163 de março de 2011[119], da UE, notam-se parcerias criadas com os EUA, G8, OCDE, CCDCOE da NATO, ITU, ASEAN[120] (UE 2011, *passim*). A salientar ainda a estreita relação de cooperação entre a UE e o COE nestes domínios, nomeadamente no âmbito do Projeto Global sobre o Cibercrime anteriormente referido (COE 2012b, 1). O ponto de partida desta estreita relação é o Memorando de Entendimento entre o COE e a UE, assinado em maio de 2007, em Estrasburgo, que desde logo no seu ponto 26 prevê o "desenvolvimento de formas apropriadas de cooperação em resposta aos desafios que a sociedade Europeia enfrenta, e a melhorar a segurança de indivíduos, particularmente no que se refere a combater o terrorismo, crime organizado, corrupção, lavagem de dinheiro e outros desafios modernos, incluindo aqueles que provêm do desenvolvimento das novas tecnologias"[121] (COE/UE 2007, 5).

A intenção geral da União traduz-se na seguinte citação:

> A Comissão continuará a desempenhar plenamente o seu papel garantindo que os Estados-Membros coordenarão a sua acção noutras instâncias internacionais em que a questão da cibercriminalidade está a ser discutida, tais como o Conselho da Europa e o G8. As iniciativas que a Comissão tomar a nível da União Europeia terão devidamente em conta os progressos alcançados noutras instâncias internacionais, embora procurando uma aproximação no âmbito da União Europeia (UE 2000, 36).

[118] *Vide* UE 2010c.
[119] *Vide* UE 2011.
[120] *Vide* nota 79.
[121] Tradução nossa.

A aproximação no âmbito da UE é óbvia em sede da Estratégia de segurança Interna, no entanto são demasiadas as referências desta relativamente à prossecução de uma política de Cibersegurança global.

II.3.3. ENISA

A ENISA foi crida através do Regulamento n.º 460/2004 do Parlamento Europeu e do Conselho, com a finalidade de

> garantir na Comunidade um nível de segurança das redes e da informação elevado e eficaz e com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público da União Europeia, contribuindo assim para o normal funcionamento do mercado interno. (PE 2004, 4)

Este documento institui a ENISA com o objetivo de reforçar a capacidade da União, dos países da UE e do setor das empresas no que diz respeito a prevenção, resposta e gestão de problemas ligados à segurança das redes e da informação. Do mesmo modo prevê-se que esta ofereça assistência e aconselhamento em trabalhos técnicos preparatórios para atualização e elaboração da legislação da UE relativa a estas temáticas (*ibid.*, *passim*).

Tem ainda por missão facilitar e incentivar a cooperação entre os intervenientes nos setores público e privado, sendo que, enquadrando-se infalivelmente na dimensão externa da União, tem por missão "contribuir para os esforços comunitários de cooperação com países terceiros e, se necessário, com organizações internacionais" (PE 2004, 3).

Note-se que em 2009, foi feita uma avaliação da ENISA, através da Comunicação 2007/285[122], onde se lê que a criação da agência se justifica, no entanto "as actividades da Agência parecem ser insuficientes para atingir o alto nível de impacto e o valor acrescentado pretendidos e a sua visibilidade é inferior às expectativas". Ainda assim e a prorrogação do mandato[123] da agência é defendido pelo que a extinção da mesma "representaria uma importante oportunidade perdida para a Europa e teria consequências negativas para a segurança das redes e da informação e o bom funcionamento do mercado interno", defendendo-se por último uma mudança da "orientação estratégica e estrutura da Agência" (ComE 2007b, 5). Amado da Silva, no mesmo sentido, caracteriza a abordagem da ENISA como "algo desequilibrada, privilegiando os sistemas e quase esquecendo as redes" (2010, 79).

[122] Vide ComE 2007b. Note-se que no texto deste documento se salienta que à data da avaliação apenas tinha decorrido um ano desde a sua entrada em funcionamento.

[123] Após esta avaliação do PE em 2008 através do Regulamento (CE) n.º 1007/2008, o mandado da ENISA foi prorrogado até março de 2012 que por sua vez foi prorrogado até setembro de 2012 por força do Regulamento (UE) n.º 580/2011 do Parlamento Europeu e do Conselho de 8 de junho de 2011.

Perante tais hesitações quanto à ENISA, somos da opinião de que esta Agência tem sido marcante no estabelecimento de um ambiente de Cibersegurança Europeu. Note-se que existem possibilidades em estudo para a ENISA relativas à alteração do formato organizacional[124]. É ainda de louvar o trabalho desta agência relativamente à cooperação entre as equipas de resposta de emergência a incidentes de segurança informática, de designação CERT[125]. Sendo que esta serve de "interligação com uma rede de equipas de emergência nacionais/governamentais de resposta no domínio informático" (UE 2010b, 10). Os CERT estão realmente articulados e são efetivamente capazes de cessar um ataque, no entanto a sua atuação situa-se no encalque ou após a ocorrência de um ataque informático, e regra geral estão instalados em Universidades e/ou empresas.

Para terminar apresentamos uma iniciativa de relevo[126] desta agência:

> O primeiro exercício pan-europeu sobre incidentes de grande envergadura a nível da segurança das redes (Cyber Europe 2010) realizou-se em 4 de Novembro de 2010 e nele participaram todos os Estados-Membros, dos quais 19 activamente, e ainda a Suíça, a Noruega e a Islândia. Será sem dúvida vantajoso que os futuros exercícios pan-europeus no domínio da cibersegurança disponham de um quadro comum baseado nos planos nacionais de emergência que garanta a articulação dos mesmos, fornecendo assim os mecanismos e procedimentos de base para as comunicações e a cooperação entre os Estados-Membros (UE 2011, 6).

"O objetivo do exercício foi acionar a *comunicação* e *colaboração* entre países da Europa para tentar responder a ataques de larga escala"[127] (ENISA 2011a, 6). O exercício, no âmbito dos CERT, foi considerado excelente, uma boa iniciativa a repetir[128]. No seguimento deste exercício realizou-se ainda um outro exercício denominado "Cyber Atlantic 2011", realizado entre a UE e os EUA (ENISA 2012a, *passim*).

II.4. Conclusão Capitular

Nítidos são os vários esforços por parte dos diversos organismos internacionais que não poupam esforços na vontade de criarem estruturas coletivas capazes de fazer face às ameaças. As movimentações estratégicas de Cibersegurança ganham solidez, dado o longo caminho que já se tem vindo a percorrer. A harmonização legislativa

[124] Vide UE 2010d, p.7-8.

[125] CERT do inglês "*Computer Emergency Response Team*". Não nos debruçaremos sobre estas equipas em particular dado o cariz reativo que estas envolvem, estas equipas atuam em caso de resiliência e resposta a ataques. Não olvidamos contudo a importância das mesmas na prossecução de uma efetiva Cibersegurança.

[126] Mais exemplos deste tipo de exercícios é o "*Cyber Storm*" realizado, bienalmente, pelos EUA; ou os "*Cyber Coalition*", "*Baltic Cyber Shield*", "*Locked Shields 2012*" do CCDCOE da NATO (apêndice n.º 11).

[127] Tradução nossa.

[128] *Vide* o relatório de avaliação em ENISA 2011a.

também faz parte do discurso que ressente as inúmeras dificuldades que jazem na transnacionalidade do espaço inerente às ameaças em questão.

Os esforços, a nível global, para que neste espaço incorpóreo reine a ordem e segurança obrigam à cooperação e empenho quer regional quer internacionalmente. Obrigação aliás impelida pelo impacto demasiado nocivo do Cibercrime junto do Estado que já se apercebeu da ineficácia da sua isolada atuação, onde quer as estruturas Estaduais quer as Interestaduais *per si* enfrentarão o insucesso num combate onde a cooperação multilateral (sem fronteiras de qualquer natureza) global se assume como a arma mais eficaz contra o Cibercrime.

III. COOPERAÇÃO POLICIAL INTERNACIONAL PERANTE O CIBERCRIME

III.1. EUROPOL

III.1.1. CRIAÇÃO E EVOLUÇÃO

A ideia que sustentou a criação da Europol foi o combate à criminalidade internacional. O conceito de uma estrutura de Polícia Europeia remonta a uma proposta de Helmut Kohl, versada numa moção apresentada no CEur do Luxemburgo em 1991, que visava a criação de uma Unidade Europeia de Polícia Criminal destinada a combater a criminalidade internacional e europeia (Farinha 2005, 440). A Europol foi, contudo e efetivamente constituída com a previsão, no Artigo k.1, ponto 9 do Título VI[129] do Tratado de Maastricth, 1992:

> A cooperação policial tendo em vista a prevenção e a luta contra o terrorismo, o tráfico ilícito de droga e outras formas graves de criminalidade internacional, incluindo, se necessário, determinados aspectos de cooperação aduaneira, em ligação com a organização, à escala da União, de um sistema de intercâmbio de informações no âmbito de uma Unidade Europeia de Polícia (Europol) (UE 1993).

O primeiro passo que o CEur tomou concertante à cooperação policial europeia foi a criação da Unidade de Drogas da Europol, cujo mandato foi todavia expandido para outras áreas de criminalidade transnacional, incluindo o terrorismo, crime relativo a veículos automóveis e crime organizado, sedimentando-se desta feita o caminho desta estrutura. O passo seguinte consubstancia-se na Convenção Europol de 1995[130] onde esta ganha o seu estatuto formal. Mais tarde o Tratado de Amsterdão, em 1997, define precisamente os objetivos dos EM, bem como os setores que carecem de cooperação no intuito de se garantir um grau elevado de segurança, aqui se reforçando igualmente, o

[129] De epígrafe: "Disposições Relativas à Cooperação no Domínio da Justiça e dos Assuntos Internos".
[130] *Vide* CEur 1995.

papel da Europol [131]. Este Tratado constitui uma importante etapa da cooperação policial na UE, onde o terceiro pilar é alvo de grande escrutínio com vista a aumentar a eficácia da cooperação policial[132].

A entrada em vigor do Tratado de Lisboa vem alterar o local de previsão desta instância, assim a Europol passa a estar prevista no art. 88º do Tratado sobre o Funcionamento da UE. Convém destacar que o PE e o CEur, através do alargamento do campo de aplicação do procedimento de codecisão instituído pelo Tratado de Lisboa, vêm os seus poderes legislativos alargados ao domínio da Europol, podendo desta feita por meio de regulamento, modificar a estrutura, funcionamento, competências e funções da mesma[133]. A salientar que a "Europol foi a primeira organização criada ao abrigo das disposições do Tratado da União Europeia" numa época onde "a criminalidade organizada internacional não se encontrava tão generalizada e a cooperação europeia no domínio da justiça e dos assuntos internos estava limitada" (ComE 2006, 2).

Neste sentido foram adotados três protocolos com vista a melhorar a sua eficácia. Um primeiro, em 2000 que dotou a Europol de competências no âmbito do branqueamento de capitais[134]. Seguidamente, em 2002, a Europol vê a sua presença manifesta nas Equipas de Investigação Conjuntas[135]. Na terceira e última ratificou-se o assinado em 2003, onde se contemplaram aspetos relativos ao acesso de dados contidos no Sistema de Informações da Europol, desenvolvimento da cooperação com países ou organismos terceiros, simplificação de procedimentos, remoção do prazo legal de três anos no armazenamento de dados, e a possibilidade da Europol aumentar o seu espetro de atuação relativamente a crimes que não constavam da Convenção Europol [136]. Atualmente está em vigor a Decisão do Conselho de 6 de abril de 2009[137], que veio simplificar o quadro jurídico da Europol graças à substituição da Convenção e dos subsequentes protocolos, consagrando este serviço como uma "agência da União Europeia a partir de 1 de Janeiro de 2010" (Brandão 2011, 11).

Ainda a referir que indubitavelmente os "acontecimentos de 11 de Setembro de 2001 e subsequentes catalisam o progresso das actividades da Europol (…) (recolha e partilha de informação, avaliação da ameaça, apoio a investigações operacionais,

[131] A salutar ainda os inúmeros progressos observados de Tampere (1999) a Haia (2004) relativos a uma zona judiciária europeia e ao desenvolvimento de uma área da justiça e liberadade europeia onde a cooperação policial sempre teve enfoque.
[132] Neste sentido Cfr. Farinha 2005 p.442 e ss.
[133] Neste sentido *vide* UE 2010g.
[134] *Vide* CUE 2000.
[135] *Vide* CUE 2002.
[136] *Vide* CUE 2004.
[137] *Vide* CUE 2009.

cooperação com Organizações Internacionais e Estados terceiros, novo quadro legal pós-Tratado de Lisboa)" (Brandão 2011, 2).

Interessante visão é a de Rob Wainwright que, caracterizou esta agência como sendo "uma moderna agência que ocupa um papel central no campo da cooperação policial da União Europeia", e onde o resultado se traduz num "impacto em quase 15 mil casos por ano, contra algumas das mais importantes redes criminosas ativas na Europa"[138] (*apud* Europol 2009, 7).

III.1.2. OBJETIVOS, MECANISMOS OPERACIONAIS E ATIVIDADES

A Europol, sediada em Haia, goza de personalidade jurídica, tem como objetivo "apoiar e reforçar a acção das autoridades competentes dos EM e a sua cooperação mútua em matéria de prevenção e combate à criminalidade organizada, ao terrorismo e a outras formas graves de criminalidade que afectem dois ou mais Estados Membros" vendo as suas competências abrangerem a "criminalidade organizada, o terrorismo e outras formas de criminalidade grave (…) de modo tal que, pela amplitude, gravidade e consequências das infracções, seja necessária uma orientação comum por parte dos Estados-Membros" (CUE 2009, 39). Sintetizando Davin diz-nos que

> tem por missão melhorar a eficácia dos serviços policiais dos Estados-Membros e potenciar a sua cooperação em domínios relevantes e fundamentais para todos os Estados-Membros da União (…) facilitando o intercâmbio de informações entre os Estados-Membros, recolher e analisar informações oriundas das polícias dos Estados-Membros, comunicar aos serviços competentes dos Estados-Membros as informações que lhes digam respeito e informá-los imediatamente das ligações detectadas entre os factos constituintes do crime em apreço (2007, 147).

A Direção da Europol decidiu por uma fase de estabilização do organismo e, depois de consolidação do mesmo, respetivamente na *Paris Vision* (2000) e no *Rhodes Vision* (2003) (Europol 2009, 23). Neste intuito foi ainda aprovado, em 2007, um documento estratégico que definia as prioridades, tarefas e objetivos do organismo e especificava as atividades principais do mesmo[139]:

> [na] sua actuação cruzam-se dinâmicas supra-estaduais (agência no quadro do Direito da UE, articulação com instituições supra-estaduais como a Comissão Europeia), intergovernamentais (coordenação de esforços nacionais), transgovernamentais (criação de redes de entidades dos Estados-Nacionais – funcionários de Ministérios, policias, membros dos serviços de informações) (Brandão 2011, 14-15).

[138] Tradução nossa.
[139] *Vide* Europol 2007

Os mecanismos principais são: o centro operacional 24/7 da Europol (único ponto para intercâmbio de dados), rede de 129 oficiais de ligação[140], infraestrutura de comunicação segura, Sistema de Informações Europol, Aplicação de Intercâmbio Seguro de Informações[141], sistemas de análise (análise operacional e análise estratégica), Rede Informática de Polícia Científica, Centro da UE de perícia em matéria de aplicação da lei, e por último, um regime robusto de proteção de dados (Europol 2011b*, passim*).

Quanto às atividades, estas são vastas e abarcam tradicionalmente o terrorismo, tráfico de estupefacientes, tráfico de seres humanos, imigração ilegal organizada, a destacar, e em 2010: "Operação Athena II", "Operação da Polícia da Grande Manchester", "Operação Tex", "Operação Golf", "Operação — île fantastique", "Operação Alcazar", etc.[142] (*idem, ibid.*).

Como já vimos a Europol coopera com diversos parceiros da UE, bem como com terceiros tendo por base acordos de cooperação, neste sentido o alcance global desta agência está consignado, para além dos EM, em relações estabelecidas com dezassete países não constituintes da UE, Interpol, UNODC e Organização Mundial de Alfândegas.

III.1.3. A EUROPOL E O COMBATE À CIBERCRIMINALIDADE

No que concerne à Cibercriminalidade, a Europol desde sempre teve competências no âmbito desta temática, note-se que já no texto da Convenção Europol de 1995, no seu anexo (referido no art. 2º de então) se plasmava diretamente a "Criminalidade Informática" (CEur 1995, 30). Sendo que a demais criminalidade inerente ao mandado da Europol já se sentiam as conjugações claras com casos de Cibercriminalidade[143].

O Cibercrime é considerado hoje uma área de ação prioritária da Europol (Robinson *et all*. 2012, 87 e CUE 2011a, *passim*). O primeiro trato com estas situações recua à criação no seio da Europol do Centro de Criminalidade de Alta Tecnologia em 2002 (Câmara dos Lordes 2010, 124). Note-se que este departamento da Europol, em junho de 2011, tinha afetas sete pessoas no combate ao Cibercrime sendo que estaria estimado um incremento de outras 10 (*ibid*., 86). Tal departamento tem três objetivos primordiais: facultar apoio em termos de investigação coordenando e contribuir para as investigações dos EM que inclui análise operacional, apoio forense especializado e

[140] Estes 129 oficiais de ligação correspondem aos dos respetivos EM, bem como terceiros, a salientar a permanência de 2oficiais de ligação em Washington e um na sede da Interpol em Lyon.

[141] Sistema SIENA concebido para permitir a comunicação e o intercâmbio rápidos, seguros e fáceis de informações e dados operacionais e estratégicos relacionados com a criminalidade.

[142] Cfr. para maiores esclarecimentos o Europol Review de 2010 (*vide* Europol 2011b, *passim*).

[143] Como por exemplo o Ciberterrorismo, veja-se o já retratado fenómeno da migração da criminalidade para o ambiente digital.

atividades técnicas; produzir e analisar informações; divulgar treinos e estabelecer ligações cooperativas. (*ibid.,* 87).

Em 2009, deu-se início à implementação da Plataforma de Cibercrime da Europol [144] (Europol 2010, 44-45), atualmente assente em três pilares, contemplando assim: o Sistema em Linha de Informações sobre Criminalidade na Internet (I-CROS)[145], o ficheiro de análise especializado da Europol[146] e por fim a Plataforma de Perícia Forense na Internet (I-FOREX)[147] (*idem* 2011b, 48-49). De salientar que, relativamente ao ficheiro de análise especializado da Europol, existe uma denominação específica bem como uma base de dados afeta aos mesmos, nomeadamente a "AWF Cyborg" e respetiva base de dados "Cyborg" organizada em prol da Cibercriminalidade que inclui os crimes elencados na CC (Robinson *et all.* 2012, 88).

Em 2010, o CEur convidou a "Europol a aprofundar a análise estratégica no domínio da cibercriminalidade" (CEur 2010, 23). Assim sendo foram "criados na Europol departamentos de investigação e desenvolvimento em perícia forense digital" e "uma task force europeia para o cibercrime (*European Cybercrime Task Force*, EUCTF), constituída por chefes de unidades do cibercrime da União Europeia, a Comissão Europeia e a Eurojust, com o objectivo de criar uma plataforma para gestores de investigações e procedimentos penais em matéria de cibercrime" (Europol 2011b, 48).

No intuito de contribuir para o planeamento estratégico de um Centro Europeu do Cibercrime, a Europol publicou a *iOCTA*[148], uma avaliação da ameaça relativa à criminalidade organizada facilitada pela *internet*. De referir ainda as Operações da Europol: "Lottery", "Drácula", "Funnel Web", "Venice Carnival" e "Comfort" não olvidando as demais elencadas para o ano de 2010[149] (*ibid.*, *passim*) relativamente ao combate do Cibercrime. Por último, a Europol dispõe também, desde 2010, de uma Rede Informática

[144] Esta plataforma é oriunda da proposta da Presidência Francesa da UE em 2008, na qual a Europol foi convidada a coordenar uma resposta Europeia relativa aos crimes relacionados com a *internet* criando esta plataforma (UE 2010e, 15).

[145] Trata-se de um centro europeu numa rede de pontos nacionais de informação em linha à Europol, situados nos EM e partes terceiras, onde todas as infrações registadas na Internet podem ser comunicadas e, se necessário, elevadas para um nível europeu. (Europol 2011b, 48)

[146] AWF – Analysis Work File, tem, aqui, como alvo a criminalidade organizada impulsionada pela Internet e pelas TIC, o enfoque é colocado na identificação e, por fim, no desmantelamento de grupos ativos no domínio do Cibercrime. O ficheiro de análise (AWF) é uma resposta ao pedido vindo dos EM da União Europeia de ajuda para combater o crime a nível internacional. (*ibid.*, 48-49)

[147] Consiste numa facilidade baseada num portal e abarca toda a informação não relacionada com dados pessoais/operacionais que de facto está incluída nos dois pilares supramencionados. A informação contida na I-FOREX é sobretudo relativa a melhores práticas e formação policiais e ajudará os investigadores a manter atualizadas as respetivas competências técnicas. (*ibid.,* 49)

[148] iOCTA - Internet Facilitated Organised Crime. *Vide* Europol 2011c.

[149] Cfr. os documentos "Europol Review" onde constam mais pormenores relativos a ações conjuntas e/ou operações de Cibersegurança encetadas pela Europol.

de Polícia Científica[150], o que permite uma investigação forense de excelência no âmbito da Cibercriminalidade (*ibid.*, 14-15).

Relativamente ao Centro Europeu de Cibercrime que já temos vindo a referir, anunciado pela CEur em 2010[151], propõe-se que tal centro seja criado fazendo parte integrante da Europol. Este facto prende-se com o facto de o trabalho desta ser "reconhecido pelos Estados-Membros e pelos outros interessados, incluindo a Interpol e as autoridades internacionais responsáveis pela aplicação da lei, dispondo já de competências em matéria de criminalidade informática" notando-se assim o excelente trabalho em matéria de Cibercriminalidade onde a Europol "multiplicou as suas atividades de luta contra o cibercrime" (UE 2012, *passim*).

Este centro, sob alçada da Europol, irá centrar as suas atividades em:

> i) Cibercrimes praticados por grupos criminosos organizados, em especial os que geram grandes lucros, como a fraude online; ii) Cibercrimes que causem danos graves às vítimas, como a exploração sexual de crianças online; e iii) Cibercrimes (incluindo ataques informáticos) que afetem as infraestruturas críticas e os sistemas de informação da União (*ibid.*, 4).

Terá como principais atribuições: "servir de ponto de convergência europeu das informações sobre a cibercriminalidade", "congregar os conhecimentos especializados europeus em matéria de cibercriminalidade para apoiar o reforço das capacidades nos Estados-Membros", "prestar apoio às investigações dos Estados-Membros em matéria de cibercrime" e "ser o interlocutor coletivo dos investigadores europeus de cibercrimes a nível das autoridades policiais e do poder judicial" (*ibid.*, 4-6). A constituição efetiva deste centro será a face mais ativa da Europol no combate à Cibercriminalidade num futuro bastante próximo[152].

III.2. INTERPOL

III.2.1. CRIAÇÃO E EVOLUÇÃO

A Comissão Internacional de Polícia Criminal, que surge como embrião da atual Interpol, remonta a encontros de Chefes de Polícia desde 1905 (Farinha 2005, 416). Com as vicissitudes decorrentes da II Guerra Mundial esta organização apenas prolifera com a aprovação de um novo estatuto, em 1956, de onde resultou a designação atual. A Interpol não tem um estatuto jurídico apoiado num tratado ou qualquer outro instrumento do direito internacional, não obstante deste facto, o mesmo não impediu que o

[150] O que facilita, por exemplo, a análise das redes sociais.
[151] *Vide* UE 2010b.
[152] Note-se que a "Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Estratégia de Segurança Interna da UE em Ação: cinco etapas para uma Europa mais segura" estabelece o prazo de até 2013 se estatuir este Centro de Cibercriminalidade consubstanciando-se na sua ação n.º 1 do 3.º objetivo *Vide* UE 2010b, 10.

> número de países aderentes, de Gabinetes Centrais Nacionais e se desenvolvesse, em particular a partir dos anos sessenta, com a introdução de processos automatizados de processamento de dados e posteriormente, com a informatização, a qual passou a permitir trocas de informação mais rápidas, mais actualizadas e com procedimentos normalizados (*ibid.*, 416-417)

A Interpol não tem uma base política sólida, contudo conseguiu um estatuto de organização internacional reconhecido pela ONU[153]. Desta forma a Interpol assume-se como uma Organização Internacional de Polícia, entre serviços de Polícia. Constitui-se assim como a maior organização deste tipo a nível mundial que conta atualmente com 190 países membros (Interpol 2012a).

A Interpol além das entidades dos atuais 190 países conta ainda com valiosas parcerias, como sendo a ONU, a UE, o G8 e a Organização Mundial da Saúde.

III.2.2. OBJETIVOS, MECANISMOS OPERACIONAIS E ATIVIDADES

Dever-se-á em primeiro lugar analisar o artigo 2º da Constituição da Interpol onde se observa que os objetivos desta são:

> 1-Garantir e promover a assistência mútua mais ampla possível entre todas as autoridades de polícia criminal dentro dos limites das leis existentes nos diferentes países e seguindo o espírito da "Declaração Universal dos Direitos Humanos";
> 2- Criar e desenvolver todas as instituições que possam contribuir eficazmente para a prevenção e repressão de crimes comuns.[154] (Interpol 2011a).

O art. 3º proíbe a intervenção ou qualquer atividade de caráter político, religioso, militar ou racial (*ibid.*) dotando-a assim de neutralidade e independência, caraterística inerente à distinção de organização internacional. O ideal da Interpol é "unir a polícia para um mundo mais seguro"; cuja missão se traduz no lema "prevenir e combater o crime através da cooperação policial reforçada" [155] (Interpol 2012e).

A Interpol dispõe de vários mecanismos na prossecução dos seus objetivos, a destacar os seguintes. O "I-link", que consubstancia uma aplicação dinâmica da internet de troca de informações distribuído pelos Departamentos Centrais Nacionais da Interpol cujo objetivo é assegurar dados consistentes, uniformes e acessíveis permitindo interligação de casos (*idem* 2012b, 1-2). Por seu turno o "I-24/7" traduz-se num sistema de comunicações global que liga as Polícias de todos os EM, autorizando a partilha de dados policiais e aceder às bases de dados criminais da Interpol no sistema 24/7 (*idem* 2012c, 1-2).

[153] Em 1949 a ONU reconheceu-a como uma organização não-governamental, passando a reconhecê-la em 1971 como uma organização intergovernamental (Interpol 2008, 1).
[154] Tradução nossa.
[155] Tradução nossa.

Verdelho viu, em 2008, no anterior sistema um importante instrumento para concretizar investigações, no entanto, em casos urgentes de pedidos de preservação de prova digital, a mesma não poderá ser usada dado que se aplicam as regras dos demais pedidos o que põe em causa essa mesma diligência por demasiada demora (2008, 19).

As bases de dados referidas traduzem-se em: "nominal data", "perfis ADN", "impressões digitais", "imagens de exploração sexual de crianças" "documentos roubados ou perdidos", "documentos administrativos roubados", "veículos roubados", "peças de arte roubadas", "atividades terroristas" e "armas de fogo" (Interpol 2012d). As Equipas de Resposta a Incidentes, que prestam assistência urgente ou investigação especializada e podem ser ativadas em poucas horas, são uma mais-valia em casos de crimes violentos ou catástrofes (*Idem* 2011b).

Em 2010 foram efetuadas várias operações, por todo o globo, relativamente a: tráfico de droga, criminalidade organizada, tráfico de crianças e pessoas, roubo de viaturas, crime farmacêutico, resíduos perigosos, crime de propriedade intelectual e tráfico de animais selvagens[156].

III.2.3. A INTERPOL E O COMBATE À CIBERCRIMINALIDADE

O Cibercrime figura como sendo uma área criminal de interesse para a Interpol. Khoo Boon Hui, o atual presidente desta estrutura, no seu discurso para a 80ª Assembleia-Geral do Vietname, alertou para o seguinte:

> Além de estarmos vigilantes a ameaças à segurança como o terrorismo, drogas ilegais, tráfico de pessoas, corrupção e os demais crimes tão chamados 'crimes tradicionais', devemos também estar conscientes que os criminosos estão a tornar-se mais sofisticados. Eles são rápidos a tirar vantagem dos rápidos avanços tecnológicos e da prevalência da *internet*. Tenho a certeza que concordarão comigo quando digo que o Cibercrime é por conseguinte um perigo claro e presente[157] (2011, 3).

Assim, a Interpol têm intentado um conjunto de ações que visam o combate da Cibercriminalidade. Segundo Verdelho (2008) a Interpol foi uma das primeiras instituições internacionais a organizar encontros de especialistas acerca do Cibercrime que remontam a Lyon, 1995. Note-se que o "programa de Cibercrime da Interpol se foca em treinos e operações acompanhando sempre as ameaças emergentes"[158] (ENISA 2012b, 23).

> A Interpol estabeleceu grupos de trabalho regionais na África, Ásia, América Latina e Europa. Estes grupos de trabalho consistem nos responsáveis ou membros experientes das unidades nacionais de crimes relacionados com computadores. A Interpol também organiza Conferências Internacionais acerca do Cibercrime destinadas a agências policiais ao nível global, organiza também

[156] *Vide* para maiores esclarecimentos Interpol 2011b.
[157] Tradução nossa.
[158] Tradução nossa.

> cursos globais de treino especializados em investigações no Ciberespaço.[159] (SCHJOLBERG e GHERNAOUTI-HÉLIE 2011, 57)

Foi na sua 6ª Conferência acerca do Cibercrime, no Cairo, que a Interpol sublinhou a importância da CC a nível global (ITU2009b, 96). Por outro lado o já referenciado ponto de contacto "I-24/7" é também uma mais-valia no combate ao Cibercrime. Segundo Schjolberg e Ghernaouti-Hélie (2011, 57) e a OCDE (2006, 20) este ponto de contacto foi aprovado pela Subcomissão do Crime de Alta Tecnologia do G8.

Resta-nos, por fim a devida referência ao Complexo Global para a Inovação da Interpol, onde ficará alojado o Centro Global de Coordenação e Comando, que dará apoio 24/7 aos vários EM e onde será instalado um Centro de Cibercrime e Segurança Digital (Interpol 2012f, 2). Para este último está ainda prevista a criação de uma Unidade de Inovação e Pesquisa em Segurança Digital que compreenderá uma Unidade de Cibersegurança e Cibercrime (*ibid.*, 3). Este centro que estará funcional em 2014 (Hui 2011, 3) representará a face mais visível da Interpol na luta contra o Cibercrime.

III.3. Cooperação Policial Perante o Cibercrime

Como já vimos "a cibercriminalidade é transnacional e requer uma resposta transnacional" (Sofaer 2000, ii). Os Estados "têm consciência de que a cooperação é a única via para atingir a resposta colectiva necessária ao combate das ameaças actuais" (Carrapiço 2008). Desta feita os é "principalmente o quadro policial e judicial" quem deve "olhar para a globalização como a catapulta para o reconhecimento de que o isolamento é o caminho da morte lenta ou da sobrevivência desesperada" (Valente 2009, 479).

III.3.1. Demanda de uma Posição Policial Preventiva

As dificuldades que temos vindo a enunciar não poderão deixar de almejar respostas preventivas. Iniciaremos esta fração fazendo a devida referência aos autores que consideram que o "único sistema verdadeiramente seguro é aquele que está desligado"[160] (Spafford *apud* Santos *et all* 2009, 228). Tikk concorda, sarcasticamente, com esta afirmação adiantando que "todos os navios estariam seguros nunca saindo do porto e os aviões se nunca levantassem voo"[161] (2012, 3). Concordamos com tal, no entanto o ónus da rede desligada da sociedade seria maior, idealize-se a perda social que também se encetaria. Note-se que existem "também sempre possíveis defesas" (Tibolet 2012, 5) sendo esta uma característica inerente às TIC; a "internet vai refazendo e reelaborando as suas exigências de segurança. Disso não tenhamos dúvidas. A cada

[159] Tradução nossa.
[160] *Vide* também neste sentido Denning 2003, 13.
[161] Tradução nossa.

anti-vírus um novo vírus, a cada vírus um novo anti-vírus. Tudo isto num jogo de sombras ou de espelhos" (Rodrigues 2012, 9).

Além de possível, a defesa, terá de ser encarada quanto a uma ótica de prevenção e reação atempada, que urge necessária para evitar uma escalada de tensão e conflito. Por isso o conceito de segurança, cada vez mais alargado, também prospetiva "atenção acrescida a uma filosofia preventiva e a uma visão global da evolução dos focos de insegurança internacional e das crises que deles decorrem, com o intuito de as prevenir e limitar, evitando o seu desenvolvimento para formas agravadas de conflitualidade" (Portugal 2003, 280). A prevenção e antecipação também surge no "topo das prioridades" (CUE 2010, 8) da UE.

Segundo a ITU, e em matéria de Cibercriminalidade, as estratégias deverão ser desenvolvidas para prevenir os ataques e desenvolver contramedidas, incluindo o desenvolvimento e promoção de meio técnicos de proteção, bem como adequar as leis para que as Polícias possam combater o Cibercrime eficazmente (ITU 2009b, 65).

É certo que um dos maiores desafios será a prevenção. No entanto veja-se que "'uma corrente é tão forte quanto o mais fraco dos seus elos'", assim "há que investir na proteção do elo mais fraco, o qual sem qualquer margem para dúvidas é o fator Humano" (Tribolet 2012, 5)[162]. Assim acreditamos veemente na possibilidade da prevenção deste tipo de ilícitos educando-se para a segurança virtual[163].

Como a segurança está aqui sob a égide de responsabilidade de cada um de nós, em matéria de prevenção, a solução afigura-se veemente na formação em matéria de segurança das TIC junto do utilizador. Discordamos portanto da posição do atual Ministro da Educação e Ciência Português, Nuno Crato, que pretende diminuir a carga horária da disciplina de TIC, considerando que os alunos do 9º ano já têm conhecimentos suficientes de informática (LUSA 2011)[164]. Desta feita pensamos que as alterações terão de passar, ao invés da vontade atual, pela incisão em matérias de segurança nesta disciplina, acrescentando "consciencialização de Cibersegurança ao currículo nacional de

[162] No mesmo sentido Adam Palmer e Benjamim Rodrigues consideram essencial a educação societal com vista à prevenção do fenómeno. (apêndices n.ºs 7 e 5 respetivamente). *Vide* Myriam Dunn Cavelty que não considera "a prevenção (…) possível", adiantando que temos "de aprender a viver com a insegurança de uma maneira pragmática. A criminalidade tradicional também não pode ser totalmente prevenida"[162] (apêndice n.º 10). O SIS considera que o trato da prevenção nos domínios do Ciberterrorismo, Ciberespionagem e Cibercrime estão sob a égide dos mesmos (apêndice n.º2). Tikk e Dufkova apresentam vários exemplos preventivos no ciberespaço de sucesso nas nossas entrevistas (apêndices n.ºs 9 e 8 respetivamente).

[163] Veja-se ainda, e acerca da deteção proactiva de incidentes de segurança bem como da possibilidade de defesa a Ciberataques, o relatório da ENISA "Proactive detection of network security incidents, report" que descreve as fontes externas de informação e as ferramentas de monotorização internas disponíveis e que podem ser usadas pelos CERT's (ENISA 2011b).

[164] Este será um exemplo, a criação de uma cultura nacional de Cibersegurança é urgente e transversal a todo o globo.

educação como um meio de espalhar o conhecimento aos alunos e seus familiares"[165] (ITU 2011b, 09) ao nível global. A função de sensibilização da Polícia junto da população a par das políticas de educação e formação, orientadas para matérias de Cibersegurança, tem de ser encarada como possível e eficaz estratégia de prevenção[166]. É urgente educar para a segurança, construindo-se desta feita uma Cultura geral de Cibersegurança.

A prevenção em ambientes virtuais deverá ser "o principal vector de actuação" (Tribolet 2012), discordando desta feita com uma habituação, ainda que pragmática, à insegurança inerente ao Ciberespaço[167]. A atuação policial antes da ocorrência do ilícito é e sempre será um desafio em qualquer tipo de criminalidade, no entanto a atividade da Polícia não se deverá somente situar *à posteriori* do crime, a própria sociedade aclama que efetivamente exista uma abordagem proactiva relativamente ao crime.

Veja-se que as "novas ameaças são dinâmicas. Em matéria de prevenção de conflitos e ameaças, nunca é demasiado cedo para começar" (COE 2003, 6). Assim, e como "as ameaças estão por toda a parte e a prevenção é mais benéfica do que a resposta repressiva, urge envidar esforços para que a lei e a ordem sejam mantidas" (Alves 2005, 389) através de estratégias preventivas. Estas têm de ser encetadas[168] num Ciberespaço que é já patrulhado hoje em dia pelas forças e serviços policiais por todo o mundo (Schjolberg e Ghernaouti-Hélie 2011, 59). Dufkova acrescenta que a coordenação entre o nível nacional e internacional é particularmente importante nesta temática (2012).

III.3.2. Demanda de uma Ação Policial Cooperativa

Segundo a ITU (2009b, 70), dada a natureza transfronteiriça do fenómeno este requer uma cooperação global das Polícias que têm jurisdição em todos os países afetados. Assim, o conceito de cooperação policial europeia, a encarar aqui como sendo o conceito transversal à cooperação entre os vários EM de uma qualquer estrutura internacional, que seguimos é o seguinte, que consigna

> a actuação combinada ou a assistência entre os Estados-Membros [da União], no vasto espectro que abrange a prevenção e o combate à criminalidade em geral, e, em particular a que, assumindo natureza transnacional, pode afectar vários Estados-Membros (…) tendo como objectivo último garantir um elevado nível de protecção dos cidadãos (Gomes 2005).

Este conceito também se aplicaria ao globo enquanto UE, e às restantes estruturas e organismos internacionais enquanto EM. A face mais visível da cooperação

[165] Tradução nossa.
[166] *Vide* Benjamim na nossa entrevista, que considera "o programa "e-escolas", com fornecimento "selvagem" de material e acesso à internet um dos momentos de menor lucidez" (apêndice n.º5).
[167] Vide apêndice n.º4.

policial internacional será certamente os pontos de contato dos Gabinetes e Unidades nacionais da Interpol e Europol que consubstanciam, desde já, a ideia prevista no art.35º da CC, onde as redes 24/7 são a base do combate e prevenção da criminalidade, transação de informações policiais e assistência técnico policial.

Todo este ambiente de cooperação a nível global, que se almeja, exige que a nível interno as Polícias terão de cooperar entre si de modo a reforçar a primeira. Não olvidamos que a cooperação policial interna não se esgota nas relações entre Polícias (cooperação policial interna horizontal), consubstanciando-se antes numa áurea de cooperação que se traduz no dever de cooperar com "todas as instituições (…) cujo escopo se encontra amalgamado nas tarefas fundamentais do Estado" (Valente 2009, 510) (cooperação policial interna vertical). Em ambos os casos as relações terão de ser saudáveis e sedimentadas, não permitindo o Cibercrime qualquer tipo de "'desavenças' e os atritos normais do serviço entre as várias polícias" (*ibid.*, 514).

Seguimos ainda a visão de Valente, onde apenas se deve "considerar cooperação quando a actuação policial de cooperação reveste um carácter recíproco ou mútuo, caso contrário, estaremos em uma situação de ajuda na resolução de um caso específico e pontual" (*ibid.*, 509). Caráter este que consubstancia mais uma das exigências que estas ameaças nos apresentam.

Para finalizar "uma cooperação efetiva entre as Polícias requer procedimentos efetivos relativos a aspetos práticos. A importância da harmonização de gatilhos e a necessidade de incorporar a participação no processo global de harmonização é por conseguinte, e pelo menos, uma tendência, se não uma necessidade, para qualquer estratégia Anti-Cibercrime"[169] (ITU 2009b, 10). A cooperação é assim uma "estratégia essencial à sobrevivência das instituições nacionais – cooperação interna – e das instituições internacionais – cooperação internacional" (Valente 2009, 501) onde estas se deverão interligar e cruzar em prol de uma eficaz Cibersegurança.

III.3.2.1. FORMAÇÃO POLICIAL

O papel da Europol e Interpol na formação das Polícias também é fator crítico de cooperação. Desde logo pela tecnicidade elevada associada às TIC. As investigações do Cibercrime são, como a ITU as carateriza, "únicas" (2009b, 170), o que exige maiores conhecimentos e formação das Polícias para fazer face aos desafios que as TIC colocam. "A Polícia tem de ter um entendimento avançado da tecnologia envolvida nos casos até para recolher a prova digital apropriadamente"[170] (Palmer 2012), sendo que esta prova é especialmente volátil. A formação eminentemente técnica terá de ser

[169] Tradução nossa.
[170] Tradução nossa.

regular, respeitando os avanços tecnológicos associados, pelo que a cooperação poderá contribuir para a excelência dessa mesma formação.

A formação generalizada a todas as Polícias é vital dado que todos trabalhamos inevitavelmente com TIC, respeitando o sentimento de *awareness* temos de ter incutidos valores de Cibersegurança para não fazer perigar os sistemas e redes, pessoais, das Organizações e até do próprio Estado.

Sendo "vital (…) educar as pessoas envolvidas na luta contra o Cibercrime"[171](ITU 2009b, 79), e no seguimento do já dito sobre a prevenção, a educação de qualquer Polícia (seja qual for a sua natureza), sob a égide instrumentos cooperativos, poder-se-á habilitar as polícias a contribuir para o sentimento de *awareness* junto da população sob a forma de sensibilizações[172]. Também desta feita se poderia consolidar a imagem das Polícias relativamente a estes ilícitos, encorajando a denúncia do Cibercrime, o que levaria a uma redução do fenómeno das cifras negras. A salientar aqui o papel da Academia Europeia de Polícia[173] e as várias iniciativas da Interpol. "Devemos alocar mais meios ao treino e educação da Polícia para combater o Cibercrime enquanto também se deverá continuar a educar o público acerca de assuntos de boas práticas de segurança e denúncia do Cibercrime"[174] (Palmer 2012, 6).

III.3.2.2. ESTABELECIMENTO DE PARCERIAS

Seguimos a visão de Adam Palmer que nos aponta "o setor privado e os grupos com fins não lucrativos" detentores de "um papel muito importante no que concerne à assistência das Polícias no combate ao Cibercrime"[175] (2012, 3).

O estabelecimento de parcerias entre Forças e Serviços Policiais e terceiros é indeclinável. O envolvimento de empresas, por exemplo, é inevitável no sentido em que torno delas ronda o Cibercrime, quer o alvo quer os meios a ele adjacentes. A denotar ainda a cooperação que deverá existir entre as Polícias e o meio académico, isto porque: "primeiro as instituições académicas formam os especialistas técnicos e de gestão da segurança da informação requisitados para elaborar e executar estratégias de Cibersegurança", "segundo porque as universidades acolhem as Equipas de Resposta a Incidentes Informáticos", e por último porque as "universidades lideram a pesquisa e

[171] Tradução nossa.
[172] Por exemplo, lê-se no n.º 2 do art.3º da Lei Orgânica da PSP ser sua atribuição um "contribuir para a formação e informação em matéria de segurança dos cidadãos".
[173] Quanto a esta, com base em relações de cooperação entre a primeira e a nossa escola, foi-nos dada a possibilidade de efetuar um curso online (via site da CEPOL) sobre a temática do Cibercrime, que sem dúvida alguma também enriqueceu a visão que este trabalho compreende.
[174] Tradução nossa.
[175] Traduções nossas. Veja-se neste sentido a parceria entre a Interpol e a *Microsoft*, a salutar ainda o *National Cyber Forensic Training Alliance* nos EUA (uma parceria sem fins lucrativos que serve de um centro de cooperação entre a polícia e a indústria que Adam diz ser bastante eficaz), e o *Norton Cybersecurity Institute* (Palmer 2012).

desenvolvimento de soluções de Cibersegurança fidedignas"[176] (ITU 2011b, 30). Veja-se o exemplo do desenvolvimento ou criação de "*softwares* forenses[177]".

A relação entre as Polícias e os CERT também terá se avizinha colaborativa, veja-se que a UE impôs aos seus membros que até 2012 deveriam "constituir uma equipa de emergência de resposta no domínio informático que funcione em boas condições. É importante que, uma vez criadas, todas estas equipas e autoridades policiais cooperem entre si em matéria de prevenção e resposta" (UE 2010b, 11)[178].

Deste tipo de parcerias poderá surgir a capacitação técnica das próprias Polícias, ganhando esta visão importante relevância, numa fase onde as economias se assumem frágeis, quer no desenvolvimento de novas ferramentas quer no prolongamento da vida útil dos equipamentos.

III.3.2.3. HARMONIZAÇÃO LEGISLATIVA

As consideráveis lacunas e diferenças entre as legislações dos Estados a nível global podem entravar a luta contra a Cibercriminalidade. A harmonização terá de se encetar também no domínio da cooperação Policial no sentido de se dotarem as Polícias de mecanismos e diminuírem os referidos entraves. "[As] diferenças entre as legislações e procedimentos penais nacionais podem dar origem a diferenças a nível da investigação e das acções penais, conduzindo a discrepâncias no tratamento dado a estes crimes" (UE 2010a, 4).

"Os Cibercriminosos movem-se à velocidade da luz, mas as Polícias movem-se à velocidade da lei"[179] diz-nos Adam Palmer (2012, 2). Seguimos, então a opinião de que os instrumentos legais também estes, enquanto enformadores da atuação policial dos Estados, terão de estar *à priori* devidamente harmonizados para uma efetiva luta ao Cibercrime, referindo-nos desta feita não só ao direito penal mas também às própria atribuições e competências legais das Polícias.

Aliás a eficácia da cooperação policial nestes domínios vê-se dependente desta mesma harmonização pelo que "as consideráveis lacunas e diferenças entre as legislações (…) podem (…) dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação" (UE 2010a, 12).

III.3.2.4. PONTOS DE CONTACTO

Os existentes são os da Interpol e Europol que assumem especial relevância em matéria de partilha de informações e pedidos de assistência. Segundo Verdelho "a ideia

[176] Traduções nossas.
[177] Note-se que atualmente já existem *sofware's* forenses capazes de procurar imagens de pornografia infantil nas malhas da *web* (ITU 2009b, 63), sendo que a Interpol tem este tipo de equipamento.
[178] Acerca desta temática, e dada a complexidade da questão *vide* ENISA 2012b.
[179] Tradução nossa.

de uma rede de pontos de contato, no contexto do art. 35.º da Convenção sobre o Cibercrime, nasceu do "G8 High-Tech Subgroup""[180] (2008, 12). Ambos os pontos de contacto têm associados os fins que a CC introduziu: "assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais" prevendo-se ainda "aconselhamento técnico", "conservação de dados", "recolha de provas, prestação de informações de natureza jurídica e localização de suspeitos" com a maior celeridade possível (COE 2001a, 22).

Estes serão certamente uma mais-valia no que concerne à troca de informações, no entanto esta apenas vingará se estabelecidas relações de confiança mútuas. Por intermédio destes a "assistência solicitada deve consistir, nomeadamente, em facilitar ou executar directamente medidas como a prestação de aconselhamento técnico, a conservação de dados, a recolha de provas, a prestação de informações jurídicas e a localização de suspeitos" (UE 2010a, 11).

III.3.3.Panorama Internacional da Cooperação Policial

Relativamente à efetividade da cooperação policial as conclusões têm sido moderadas. Tradicionalmente a cooperação policial está subjugada sob várias fragilidades. Valente aponta que "a dispersão e multiplicação de organismos europeus e internacionais, que ainda impera, sem um centro coordenador único, muitos deles sobrepondo-se nas competências, permite também dispersar informação fulcral para a prevenção e repressão da criminalidade em geral e do crime organizado em especial" (2009, 529).

O mesmo autor defende uma cooperação policial mais direta, (*ibid.*), pois geralmente é de natureza diferida, não olvidamos contudo a fiscalização necessária. Relativamente à cooperação no seio da UE, Gomes caraterizou a cooperação da UE como "virtual" devido a vários fatores:

> soluções normativas muitas das vezes ambíguas; (…) compromissos politicamente assumidos pelos Estados-Membros e não cumpridos na prática; (…) ordens jurídicas, modelos policiais e judiciários diversos e dificilmente compagináveis; incapacidade de resposta dos Estados-Membros às exigências da União, (…) falta de confiança mútua (…) … (2005, 485).

A própria UE tem vindo a reconhecer a debilidade da cooperação policial e judiciária, reconhecendo os progressos insuficientes neste sentido[181]. Quanto à Europol,

[180] Tradução nossa.
[181] *Vide* PE 2010 e ComE 2007c e ComE 2008.

Nabais adianta que "existem constrangimentos que limitam a eficácia do esforço cooperativo", constrangimentos interligados com

> a falta de uma cultura de partilha de informações por parte dos Estados, que para além de serem renitentes à partilha, preferem os acordos bilaterais, visto as informações serem de tal modo valiosas e sigilosas que são objecto de troca, e por se valorizar o conhecimento prévio da entidade com quem se negoceia, o que reforça a confiança e o secretismo (2011, 57).

Neste sentido Valente reafirma o "sonegamento de informação quer a nível interno quer a nível internacional" (2209, 530)[182]. O próprio mecanismo de intercâmbio de informações foi construído sob a égide preventiva das ameaças supranacionais. Já Nabais, e relativamente ao terrorismo (cuja abordagem cooperativa estará certamente muito mais sedimentada) afirmou que "existem constrangimentos que limitam a eficácia do esforço cooperativo" baseada "na falta de uma cultura de partilha de informações por parte dos Estados" (2011, 56-57). Sendo que esta é a abordagem mais próxima que nos é possível fazer em relação ao panorama da partilha de informações entre as Polícias.

Um outro constrangimento que afigura-mos desde já, decorre do facto de a Europol e a Interpol, estarem dependentes dos pontos de contacto das respetivas Polícias nacionais, daqui decorre que a burocratização possível existente entre estas prolifere e interfira assim no bom funcionamento da estrutura cooperativa global. Qualquer relação externa sofrerá ainda debilidades provenientes das questões culturais, nomeadamente diferenças sociais e de linguagem, observando-se também diferenças a nível da cultura organizacional e institucional assente na maioria das vezes no secretismo e na excecionalidade, afigurando-se como uma das fortes barreiras à cooperação (Fägerstern 2010, 504). Também este facto afeta a eficiência cooperativa da Europol [183].

III.3.3.1. (DES)HARMONIZAÇÃO LEGISLATIVA

Almejar a um planeta onde reina uma plena harmonização legislativa parece-nos utópico. Neste sentido a cooperação entre Polícias no combate ao Cibercrime apresenta-se fragilizada sendo que depende de tal harmonização. A CC apresenta sem dúvida uma boa base à cooperação internacional[184] a nível global.

---

[182] Neste sentido, e no sentido da ineficiente partilha de informações no seio da UE, *vide* Saloven 2010 e Tikk 2012 que afirma que a falta de partilha de informações de algumas jurisdições é hoje um grande obstáculo a ultrapassar.

[183] *Vide* Verdelho 2008 e Saloven 2010.

[184] Tão só pela previsão dos seguintes artigos: recolha, em tempo real, de dados de tráfego (art.20º), interceção de dados de conteúdo (art.21º); princípios gerais relativos à cooperação internacional (art.23º), extradição (art.24º), princípios gerais relativos ao auxílio judiciário mútuo (art.25º), informação espontânea (art.26º), procedimentos relativos aos pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis (art.27º), confidencialidade e restrição de utilização (art.28º), conservação expedita de dados informáticos armazenados (art.29º), divulgação expedita de dados de tráfego conservados (art.30º), auxílio mútuo para o acesso a dados informáticos armazenados (art.31º), acesso transfronteiriço a dados armazenados num computador mediante consentimento ou quando se trate de dados acessíveis ao público (art.32º), auxílio

No entanto, nesta, temática apresenta-se uma grande vicissitude que se traduz no facto de as estruturas e organismos, a nível regional e internacional, não disporem de mecanismos que obriguem, de facto e celeremente, os EM a transporem as suas decisões para a legislação doméstica. Não olvidamos as ferramentas que estas têm, nomeadamente a nível da UE o procedimento por infração, para o efeito; no entanto as mesmas não terão a celeridade a que o Cibercrime obriga[185]. O processo legislativo também terá de acompanhar o ritmo das ameaças, podendo ser por isso, perigoso a Decisão-Quadro de 2005 ainda estar em vigor na UE, intocada no seu todo, 7anos após a sua criação[186].

Verdelho acrescenta que fora "das instituições internacionais, a coordenação pode ser mais dificultada pelas diferentes sensibilidades dos vários Estados do mundo" sendo que esta "situação é muitíssimo frequente na actualidade" (2012).

Neste sentido, Verdelho em 2008 adiantou que a falta de harmonização onde a diferença entre os sistemas legais que envolvem a preservação de dados marca negativamente o relacionamento cooperativo (2008, 30). Ainda o mesmo autor constatou, reforçando o aqui jorrado, que "diferentes tipos de incriminação, diferentes procedimentos e diferentes regras nas jurisdições (…) criaram dificuldades para a cooperação internacional"[187] (2008, 25). Surge do mesmo modo necessário envidar esforços concretos neste âmbito relativo à definição concreta de conceitos e definições relacionados com a temática, para que a harmonização seja o mais completa possível.

O caráter de mutação de excelência que o Cibercrime enceta também não permitirá hesitações quanto à produção legislativa atualizada, prevendo-se desta feita, e sob o exemplo da não atualização da Decisão-Quadro 2005/222/JAI até à data, mais um condicionante da atividade policial.

III.3.3.2. EFICÁCIA E EFICIÊNCIA DOS PONTOS DE CONTACTO

Verdelho que no seu estudo[188] contemplou as práticas de três países, nomeadamente França, Roménia e Estónia (Países Membros das redes quer do G8,

mútuo para a recolha, em tempo real, de dados de tráfego (art.33º), auxílio mútuo para a interceção de dados de conteúdo (art.34º), e por último a rede 24/7 (art.35º) (COE 2001ª, *passim*).

[185] A título de exemplo Portugal transpôs a Decisão-Quadro n.º 2005/222/JAI apenas quatro anos mais tarde, sendo que o prazo de 16 de março de 2007 foi negligenciado em dois anos. Dois anos de evolução tecnológica e Cibercrime têm muito impacto. A própria cooperação policial entre Portugal e os restantes parceiros encontrou-se comprometida neste espaço temporal. Foi também, e somente em 2009 que Portugal adaptou o direito interno à CC.

[186] Neste sentido, encontra-se em discussão a proposta da UE de 2010 (*vide* UE2010a), e somos da opinião que mesmo esta proposta tardou em figurar na discussão da União.

[187] Tradução nossa.

[188] Atente-se que este estudo data de 2008. A realidade de hoje já conta com quatro anos de evolução que nestas matérias é colossal.

quer da Interpol e Europol)[189], revela que os pontos de contacto 24/7 nem sempre responderam a pedidos ao abrigo do art. 29º da CC, o que revelou uma falta de eficácia dos mesmos, ainda revelando a vicissitude que a França divulgou, que subsiste no facto do idioma das redes 24/7 não facilitar a cooperação (2008, 35).

Benjamim refere, relativamente aos pontos de contacto que "o problema da cooperação internacional está sempre dependente da "benesse" do Estado demandado" sendo que "os nacionais agarram-se (ou tendem a agarrar-se) à "saia da mãe-pátria". Esta constatação pode levar a níveis de inoperacionalidade" (2012). Mais uma vez a dependência dos EM (quando esta não se rege pelo profissionalismo) infetará o global.

O lado burocrático da assistência mútua internacional também é deficitário em termos de proficiência, quando o implacável Cibercrime entra na equação, pois os "requerimentos formais e o tempo necessário para colaborar com Polícias estrangeiras por vezes atrapalham as investigações"[190] (ITU 2009b, 70), sendo que esta será a opção se os pontos de contacto não responderem. Os 60 dias previstos no n.º 7 do art. 29º da CC sob a epígrafe da preservação expedita de dados informáticos armazenados também se revelaram escassos segundo Verdelho (2008, 30) pelo que afiguramos o Cibercrime não permita que este prazo seja suficiente[191].

Quanto à resposta dos pontos de contacto, afigura-mos que a nível internacional a mesma deveria ser obrigatória, pelo menos nas condições que a UE[192] prevê, e que se traduz numa imposição de resposta versada na lei onde a resposta teria de ser dada "no prazo máximo de oito horas[193]" onde deve constar "pelo menos (…) de que forma e quando será atendido o pedido de ajuda" (UE 2010a, 17). Adiantamos também que o não cumprimento deste prazo deveria ter uma qualquer repercussão punitiva. Acreditamos que apenas desta forma a eficácia e eficiência deste mecanismo estaria garantida.

III.3.3.3. POLÍCIA, PARCERIAS E MEIOS

As relações com o setor privado deveriam, a nosso ver, ser reforçadas por parte das tutelas sob um prisma de exploração profícua para ambos. Desde logo sob a égide da prossecução do interesse comum adotando-se a obrigatoriedade, imposta por lei, de as mesmas fornecerem dados às Polícias na prossecução de investigações conforme art. 20º e 21º da CC[194]. Uma débil cooperação entre a Polícia e o ramo privado coloca em

[189] Para razões mais exaustivas acerca da escolha destes três países de excelência cfr. pág20 do estudo em questão. Ref. Bibliográfica Verdelho 2008.

[190] Tradução nossa.

[191] A Decisão Quadro 2005/222/JAI, em vigor na UE, nada adianta sobre estes prazos.

[192] *Vide* UE 2010a.

[193] Relativo a pedidos urgentes. Note-se que somos da opinião que o próprio conceito de urgência teria de estar explícito para se evitarem interpretações "criativas" dos Estados.

[194] No sentido de obrigar um prestador de serviços, no âmbito da sua capacidade técnica a cooperar com as autoridades competentes e a dar-lhes assistência na recolha ou no registo, em tempo real, dos dados

causa o combate das ameaças. Tribolet alerta para o facto de ser "necessário criar mecanismos que facilitem a cooperação entre o sector privado nacional e internacional, promovendo as empresas nacionais a estarem presentes nos principais fóruns internacionais nos aspetos de prevenção e resposta a incidentes" (2012, 2).

Sendo necessário portanto que "as empresas compreendam que a segurança da sociedade deve estar acima dos seus interesses particulares e que um sistema de maior partilha de informações só as poderá beneficiar a longo termo" (Carrapiço 2005, 188). Adiantamos que o estabelecimento deste tipo de parcerias deveria estar derramado nas orientações estratégicas dos Estados a nível global, bem como a obrigação legal das mesmas fornecerem dados às polícias. É Hui (2011, 3) quem alerta para o facto de o sucesso deste confronto com o Cibercrime residir numa abordagem holística que envolve as partes interessadas e os setores privado e público.

Quanto aos meios, torna-se "crítico que as Polícias estejam autorizadas a investigar e perseguir o Cibercrime eficazmente, sendo que estas necessitam dos meios e instrumentos necessários para investigar o Cibercrime"195 (ITU 2009b, 13-14). Afiguramos que os meios técnicos não serão os mais adequados na medida em que os meios tecnológicos terão de seguir a evolução incessante das TIC, o que se torna demasiado oneroso, nem sempre se permitindo com a urgência necessária substituir e/ou atualizar as ferramentas, pelo que "os meios tecnológicos nunca serão suficientes" (Morgado 2012, 2). Já vimos as vantagens deste tipo de parcerias, no entanto Tribolet (2012) afirma que a cooperação entre polícia e indústria é escassa a nível internacional.

O crescente número de utilizadores das TIC, particularmente da *internet,* também trará problemas às Polícias relativos aos meios humanos que são escassos[196]. Para já porque é "relativamente difícil automatizar o processo de investigação" (ITU 2009, 66) baseados em *sofwares* forenses, pelo que a componente humana terá de ser reforçada, desta feita já com a devida formação técnica. Por outro lado é utópico a ideia de ter um polícia ao lado de cada criminoso, sendo que assim o crime nunca vingaria. Aliás o Ciberespaço dificulta o agora dito[197]. Tornando-me repetitivo, e no seguimento do já referido acerca de *software's* forenses, a indústria e os meios técnicos que poderão facilitar, também teria impacto a nível dos meios humanos.

---

de conteúdo de comunicações específicas feitas no seu território, transmitidas através de um sistema informático. (subalíneas ii) das alíneas b) do n.º1 do respetivo artigo).

[195] Traduções nossas.

[196] Neste sentido aponta o já referido acerca da Europol que comporta apenas sete pessoas no Centro de Criminalidade de Alta Tecnologia, sendo que o incremento de mais 10 pessoas ajudará caso se confirme.

[197] E note-se que este polícia teria de ter a devida formação técnica, pois o seguimento deste fenómeno assim o exige.

Quanto à falta de estatística fiável, esta torna-se nefasta para a atividade policial e consequente cooperação na medida que se desconhece em certa parte o fenómeno que se pretende enfrentar. Partilhando assim da opinião da ITU (2009, 62) quando adianta que o acesso a informação mais precisa acerca da verdadeira incidência do Cibercrime iria ajudar as Polícias a: melhor perseguir os ofensores, deter potenciais ataques e a desenvolver legislação apropriada e efetiva[198].

Sentimos que "[a] Polícia faz um ótimo trabalho na tentativa de travar o Cibercrime, no entanto o problema requer significativamente mais meios do que os que estão a ser orientados para para-lo"[199] (Palmer 2012).

III.3. Conclusão Capitular

Configuramos o Cibercrime como o mais transnacional de todos os crimes. Para um eficaz controlo do Cibercrime urge uma cooperação policial internacional sem hesitações que será profícua. Têm vindo a ser identificadas algumas fragilidades inerentes à cooperação Policial, via Europol e Interpol, entre os Estados da UE. No entanto, como já vimos, têm vindo a ser encetados esforços de grande impacto e valor acrescentado relativamente a esta área, não estando o Cibercrime certamente à derida e sob o controlo de criminosos (não na sua totalidade).

O trabalho da Europol e Interpol não é desprezível, e tem sido bem coordenado (Benjamim 2012), sendo que esta já se traduz em si mesma um fórum muito poderoso de cooperação global (Palmer 2012)[200], este trabalho muito tem sido deveras importantes, embora ainda não perfeito (Cavelty 2012). "A natureza intrínseca da cooperação criminal (que tem sempre na base acordos voluntários entre Estados) não potencia a coordenação entre os diversos actores – maxime os Estados -, fora dos quadros institucionais" (Verdelho 2012). Tal facto sempre fragilizará a cooperação policial.

Temos contudo a noção da importância e necessidade da cooperação internacional a nível geral, conforme afirmaram todos os nossos entrevistados. Assim, ousando adaptar a expressão de Brandão afirmamos que: o globo "corre o risco de ter as notas musicais, mas nunca a melodia"[201] (Brandão 2003, 186) que se exige contra o Cibercrime.

---

[198] A nível da UE já se está a tratar de orientar as políticas no sentido da existência de dados deste género (UE 2010a), o documento que prevê a revogação da Decisão Quadro 2005/222/JAI já prevê no seu art. 15º "a existência de um sistema para o registo, produção e disponibilização de dados estatísticos sobre as infrações" que temos vindo a tratar.

[199] Tradução nossa. No mesmo sentido Tikk na sua entrevista revela esta falta de meios de algumas jurisdições como um dos grandes obstáculos a ultrapassar atualmente (*vide* apêndice n.º 9).

[200] Tikk também considera estes, e atualmente, uns dos mais efetivos relativamente à cooperação a nível geral (apêndice n.º 9).

[201] Brandão faz esta afirmação em relação à União (*vide* Brandão 2003, 186).

Hert, Fuster e Koops (2006, 524) adiantam que é provavelmente irrealista expectar que um dia haverá consenso relativamente a todas as medidas necessárias para lidar com o Cibercrime.

CONCLUSÃO

CONCLUSÕES SOBRE AS HIPÓTESES E A PROBLEMÁTICA

Muito foi já discorrido acerca da sociedade e das ameaças. O uso indevido das TIC é real. A sociedade é, de facto, cada vez mais digital. O impacto destes factos é assolador e as dificuldades que emergem para os Estados, imensas. É este o panorama que desenhamos no nosso trabalho, contudo não devemos ser pessimistas ao ponto de considerar que não existe forma de combater e prevenir o Cibercrime. A trave mestra de tal afirmação consigna-se numa e tão só palavra, cooperação. Sendo que a *internet* não é, nem pode em momento algum configurar-se, como um *off-shore* judicial e policial onde os criminosos tenderão a refugiar-se.

As ameaças transnacionais são cada vez mais virtuais bem como os crimes tradicionais aos quais o Estado estava já acostumado. As inclinações estratégicas de segurança, que foram escortinadas, revelam claramente a tendência para o alargamento do conceito de segurança, revelando também a perceção que o Estado adquiriu da incapacidade da sua erma atuação. Não se têm poupado esforços, a nível internacional, para criar instrumentos eficazes e coordenados que permitam diminuir o Cibercrime. Os instrumentos que têm sido orientados para o fenómeno, que apresentamos, são prova disso.

A atuação policial tem inevitavelmente seguido o mesmo destino. Vários são os exemplos apresentados. As operações conjuntas da Europol e Interpol em matéria de Cibercriminalidade são reais e frutuosas. As próprias estruturas internas têm vindo a reorganizar-se, criando mecanismos próprios de combate à Cibercriminalidade. Expoente máximo dessa direção é a previsão da criação do Centro Europeu de Cibercrime na égide da Europol e o Centro de Cibercrime e Segurança Digital da Interpol. A própria cooperação policial é alvo de sucessivos melhoramentos.

A certeza subjaz contudo em dois vetores: num claro aumento da atividade Cibercriminosa; e nos novos desafios que as Ciberameaças colocam à atividade das forças policiais que, neste ambiente, surge fragilizada pela essência virtual do Ciberespaço. Não obstante dos inúmeros avanços nesta matéria destes esforços conjuntos, continuam a existir fragilidades decorrentes das relações entre os EM e as estruturas internacionais. Do Ciberespaço em si emanam desafios espinhosos.

Desde já a profetização de um globo unido, harmonizado de tal maneira que não restem dúvidas quanto à capacidade dos Estados enfrentarem as Ciberameaças, parece-

nos deveras utópica. *Ab initio* pelas incontornáveis e subjacentes questões culturais, económicas e sociais que sedimentam o caráter utópico que afirmamos. Este facto coloca inúmeros desafios não só às relações internacionais entre EM, mas também e *per si* à cooperação policial. Note-se que qualquer relação que envolva os níveis nacional e internacional estará sempre subjugada reciprocamente. Qualquer tipo de atrito nestas relações terá repercussões no sistema global.

O argumento central de investigação que formulamos vê-se em certa medida confirmado, constatadas as tradicionais debilidades da cooperação policial que há muito vêm a ser identificadas. Estão, de facto, inerentes a este tipo de relações obstáculos que perigam desde logo por se apelidarem de tradicionais. Voltando desde cedo às questões inerentes a cada uma das sociedades onde os pontos de contacto Europol e Interpol operam. A própria cooperação está, desde logo condicionada, pelo empenho pessoal e organizacional da Polícia que recebe um qualquer pedido de cooperação. As Ciberameaças são demasiadamente implacáveis não permitindo qualquer tipo de atritos, rivalidades ou condicionantes entre os serviços policiais, quer a nível nacional quer a nível internacional.

As estruturas e os instrumentos de cooperação policial internacional não promovem uma coordenação eficaz no combate e na prevenção global do Cibercrime. Tão só pelo facto de não haver uma coincidência exata entre os EM pertencentes à rede da Europol e Interpol bem como à rede 24/7 do G8. Aos próprios pontos de contacto estão adjacentes falhas correlacionadas com a não resposta e com a dificuldade que os diferentes idiomas apensam à equação. Quando tal se verifica, os despoletados tradicionais pedidos de assistência mútua tendem a ser incapazes nestas matérias. A burocracia inerente não corresponde de facto à urgência destas matérias: idealize-se um pedido de preservação de dados “perdido” por entre cartas rogatórias que, apesar de respondido, poderá não alcançar a essência do mesmo (tal é a volatilidade do meio de prova). O mais perto que nos foi possível chegar a esta temática foi através de um estudo de 2011 onde as fragilidades e constrangimentos destes pontos de troca de informações e relativamente ao terrorismo, foram também identificadas.

A nível da harmonização legislativa, que a nível global já se nos afigurou utópica, urge legislar melhor no sentido da objetividade e atualização dos quadros legais internacionais. A necessidade de quadros legais homólogos, em matéria de Ciberameaças é uma urgência que não admite hesitações. O panorama atual ainda se encontra longe do que realmente é pretendido perante as exigências do Cibercrime. A objetividade desta ação surge a par da capacidade “criativa” dos EM na interpretação da lei, sendo que por outro lado, a atualização terá de responder a este fenómeno de

mutação acelerada. Enquanto este quadro não se verificar a cooperação e atividade policial estarão deveras comprometidas.

Veja-se a lei como o referencial balizador e enformador da função policial. É necessário atentar aos quadros legais sob um ponto de vista de harmonização que crie condições favoráveis ao trabalho da Polícia. Trabalho esse que não poderá certamente ver-se comprometido por o artífice, astuto, do Cibercrime se colocar sob a égide de paraísos legais onde a ação da Polícia é dificultada ou até impossível. Os regimes de preservação e acesso a dados também terão de ser alvo nesta harmonização para que se garanta o meio de prova. Os próprios poderes policiais também estes terão de ser comuns. Neste momento a desarmonização sente-se *ab initio* pelas dificuldade dos organismos internacionais efetivarem célere e prontamente as suas decisões em matéria de Cibercrime, pois não haverá lugar para processos de incumprimento case impere a urgência.

É também urgente a formação da Polícia nestas matérias. Têm de ser adotadas estratégias de formação para os elementos Policiais, sendo que sentimos esta escassez na nossa própria formação relativamente a estas temáticas. A formação da Polícia em consonância com políticas de formação e educação governamentais são particularmente proveitosas em sede de prevenção. Desde logo a posição privilegiada da Polícia junto do cidadão clama esta necessidade em jeito de ações de sensibilização e formação.

Face às fragilidades dos meios técnicos e humanos inerentes a tão complexo fenómeno, urge também dotar as Polícias de meios capazes que se afiguram imortalizados na insuficiência que jaz junto da evolução constante das TIC. Aqui, o número de sete pessoas alocadas (em 2011) na estrutura relativa ao Cibercrime da Europol padecerá fragilizado no sentido de resposta célere a toda a União. As parcerias Público-Privadas apresentam-se de tal maneira profícuas que não haverá espaço para a rejeição das mesmas.

A Interpol, por seu lado, enfrentará desafios acrescidos dado não ter uma base política como a Europol, onde em pano de fundo surge a União configura uma *polity* com capacidade de elaboração e implementação de políticas. Também é certo que os meios quer humanos, quer técnicos; tenderão à escassez tal é a evolução constante das TIC que o próprio crime acompanha.

Os instrumentos e estruturas estão criados de facto, no entanto, a sua eficácia é limitada pelo défice de coordenação dos mesmos. Esta é a própria visão que a UE tem vindo a confirmar. A atividade policial vê nos seus pontos de contacto da Interpol e Europol, uma importância sem igual face aos do Cibercrime. A urgência que destes transpira vê nos pontos de contacto um instrumento facilitador de cooperação internacional. Subjacente a estes pontos de contacto está essa mesma urgência bem

como o cariz de assistência mútua expedita que o Cibercrime exige. Este último poderá certamente sair derrotado no confronto com esta ferramenta de cooperação internacional, na medida em que estes funcionem em termos de eficácia e eficiência, respondendo em igual moeda aos implacáveis ataques virtuais.

A cooperação entre Polícia e Indústria é inevitável, nesta última ronda o Cibercrime (alvo e meios) bem como o *empowerment* das ferramentas policiais. A tecnicidade subjacente, bem como o desenvolvimento acelerado das TIC, em consonância com o estabelecimento de Parcerias Público-Privadas, poderá permitir a melhoria da capacitação técnica das Polícias. Sendo certo que referimos apenas as relações de "cordialidade", havendo ainda espaço para as relações impostas por lei, nomeadamente em determinadas obrigações relativas aos fornecedores de serviços das TIC. O envolvimento de empresas privadas ou públicas assume-se elementar em matérias de desenvolvimento, substituição e até reparação das ferramentas policiais.

Por outro lado a aposta terá de passar indubitavelmente pela criação de uma cultura de Cibersegurança, através da educação e formação em segurança virtual. E sendo que a formação de todo e qualquer Polícia nesta área é necessária, urge envidar esforços para se estabelecerem relações com o meio académico. Como vimos poderão advir incrementos nas próprias ferramentas policiais. Torna-se crítico criar um ambiente de *awareness* relativamente ao uso das TIC. Adjacente ao meio académico estará também a potencialidade de investigação que também aqui é profícua. Este pensamento ganha justificação nesta fase onde as economias estaduais são frágeis.

Sendo certo que a cooperação policial internacional nestas matérias tem de ser encarada em dois níveis: *ab initio* a nível nacional entre as diversas Forças e Serviços de Segurança, sendo que *à posteriori* poder-se-ão sedimentar as relações externas. A ação policial em si encontra-se desta feita comprometida diante de um empenho indevido, desde logo, a nível nacional.

Os mecanismos estão criados, bons exemplos foram já observados. Não que se torne necessário um primeiro passo nesta caminhada, pois esta está em curso, no entanto a direção terá de ser alinhada no sentido de aprimorar as estruturas e ferramentas de cooperação policial já existentes. O caminho está traçado, a caminhada iniciada, no entanto sentimos que ainda muito falta percorrer nesta senda de cooperação exímia a que o estado de Cibersegurança obriga.

IMPLICAÇÕES POLÍTICAS E PRÁTICAS

Em síntese, destacamos: acriação de mecanismos, a nível das Organizações Internacionais, que em casos de alterações dos quadros legislativos dos EM relativos a Ciberameaças lhes permitam efetivar com celeridade a transposição dessa mesma alteração; o empenho por parte dos EM em adotar decisões das instâncias

internacionais, e por seu lado empenho por parte das instâncias internacionais em legislar qualitativa e objetivamente; a obrigatoriedade de resposta, perante matérias transnacionais, por parte dos pontos de contato, imposta na lei e com mecanismos de punição para o seu não cumprimento; a adoção de políticas de educação e formação em Cibersegurança, Estaduais (cidadão) e organizacionais (polícia); a formação vincada nesta área nas escolas de formação da nossa Polícia em concreto.

LIMITAÇÕES DA INVESTIGAÇÃO

O processo de investigação confrontou-se com as seguintes dificuldades: (in)definição de conceitos; défice de dados estatísticos (comparáveis); impossibilidade de realizar entrevistas junto da Polícia Judiciária e suas estruturas (Diretor-Nacional da PJ, Unidade de Cooperação Internacional da PJ e consequentes: Unidade Nacional da Europol e Gabinete Nacional da Interpol; e Unidade de Telecomunicações e Informática da PJ).

CONTRIBUTOS PARA UMA POSSÍVEL INVESTIGAÇÃO FUTURA

É necessário abordar esta questão sob uma dicotomia: poderemos estar perante "o regresso do Adamastor" onde a "privacidade encontra-se a saque" (Rodrigues 2009, 114), "a era digital não é nem o «big brother» nem o «ciber-oeste selvagem»" (UE 2010c, 18). Concluímos com sugestões para uma futura investigação: avaliação da cooperação judiciária nesta temática, dada a aproximação à Polícia; estudo dedicado ao impacto das parcerias Público-Privadas na Cibersegurança; análise da relação entre Polícia e CERT, (um estudo aprofundado seria proveitoso considerando as díspares naturezas que os envolve, afigurando-se demasiadas limitações); estudo sobre a prevenção por intermédio da formação; estudo comparado (entre EM) dos mecanismos de coordenação interníveis (nacional e europeu) no combate ao Cibercrime; estudo acerca da adaptação do atual Programa Integrado de Policiamento de Proximidade (PIPP) ao Ciberespaço; aferição de medidas de Ciberpoliciamento.[202]

"***Summo rigore***, *não podemos ser avestruzes e esconder a cabeça na areia como se nada girasse à nossa volta, como se o mundo fosse o 'eu' do 'nós' sem que ao nosso lado estivesse(m) o(s) 'outro(s)'*"[203].

[202] Texto escrito conforme o Novo Acordo Ortográfico - convertido pelo Lince.
[203] Manuel Monteiro Guedes Valente (2009, 530). Grifo e itálico nosso.

Lisboa, 26 de abril de 2012

Nélson Tiago Carvalho Silva
Aspirante a Oficial de Polícia

BIBLIOGRAFIA

FONTES PRIMÁRIAS

PORTUGAL, Assembleia da República. 2003. "Lei do Cibercrime". Lei nº109/2009 de 15 de setembro. *Diário da República*: I Série, Nº179.
Disponível em: *[http://dre.pt/pdf1s/2009/09/17900/0631906325.pdf]*

_____, Presidência do Conselho de Ministros. 2012. "Resolução do Conselho de Ministros n.º 12/2012 de 07 de fevereiro de 2012". *Diário da República*: I Série, Nº27.
Disponível em: *[http://dre.pt/pdf1sdip/2012/02/02700/0059600605.pdf]*

_____, Presidência do Conselho de Ministros. 2003. "Conceito Estratégico de Defesa Nacional, Resolução do Conselho de Ministros n.º 6/2003". *Diário da República* N.º 16, Série I-B, de 20 de Janeiro: 279-287.
Disponível em: *[http://dre.pt/pdf1sdip/2003/01/016B00/02790287.pdf]*

CÂMARA DOS LORDES. 2010. "Protecting Europe against large-scale cyber-attacks – Report with Evidence". Londres: The Stationery Office Limited. Disponível em: *[http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf]*

COMISSÃO EUROPEIA. 2000. "Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões – Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e lutando contra a cibercriminalidade – eEurope 2002". [COM(2000)890]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:PT:PDF]

_____. 2006. "Proposta de Decisão do Conselho que cria o Serviço Europeu de Polícia (EUROPOL)". [COM(2006)817]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0817:FIN:PT:PDF]

_____. 2007a. "Rumo a uma política geral de luta contra o cibercrime - Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões". [COM(2007)267]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:PT:PDF]

_____. 2007b. "Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Avaliação da Agência Europeia para a Segurança das Redes e da Informação (ENISA)". [COM(2007)285]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0285:FIN:PT:PDF]

_____. 2007c. "Comunicação da Comissão ao Conselho e ao Parlamento Europeu – Relatório sobre a aplicação do Programa da Haia relativamente a 2006". [COM(2007)373]. Disponível em:
[http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2007)0373_/com_com(2007)0373_pt.pdf]

_____. 2008. "Comunicação da Comissão ao Conselho e ao Parlamento Europeu Relatório sobre a aplicação do Programa da Haia relativamente a 2007". [COM(2008)373]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0373:FIN:PT:PDF]

_____. 2009. "Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões relativa à proteção das infraestruturas críticas da informação – Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência". [COM(2009)149]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:PT:PDF]

CONSELHO DA EUROPA. 2001a. "Convenção sobre o Cibercrime". *Série de Tratados Europeus* n.º 185. Disponível em:
[http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf]

_____. 2001b. "Rapport explicative sur la Convention sur la cybercriminalité – STE n.º 185" Disponível em:
[http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm]

_____. 2005. "Warsaw Declaration". Declaração Final da 3ª Cimeira dos Chefes de Estado e Governo do Conselho da Europa, Varsóvia, 16-17 de maio.
Disponível em: *[http://www.coe.int/t/dcr/summit/20050517_decl_varsovie_en.asp]*

_____. 2012a. "Global Project on Cybercrime (Phase 2) – 1 March 2009 to 31 December 2011 – Final project report". Disponível em:

[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_adm_finalreport_V12_9apr12.pdf]

_____. 2012b. "Global Project on Cybercrime (Phase 3) – Project summary". Disponível em:
[http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_project_Phase3_2571/2571_Phase3_summary_V6_Mar2012.pdf]

CONSELHO DA EUROPA/UNIÃO EUROPEIA. 2007. "Memorando de Entendimento entre o Conselho da Europa e a União Europeia". Disponível em:
[http://www.coe.int/t/der/docs/MoU_EN.pdf]

CONSELHO DA UNIÃO EUROPEIA. 2000. "ACTO DO CONSELHO de 30 de Novembro de 2000 que estabelece, com base no n.º1 do artigo 43.º da Convenção que cria um Serviço Europeu de Polícia (Convenção Europol), um protocolo que altera o artigo 2.º e o anexo daquela convenção". [JO C 358 de 13/12/2000]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:358:0001:0007:PT:PDF]

_____. 2001. "Recomendação do Conselho relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia". [JO C 187 de 3/7/2001]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2001:187:0005:0006:PT:PDF]

_____. 2002. "Acto do Conselho de 28 de Novembro de 2002 que estabelece um protocolo que altera a Convenção que cria um Serviço Europeu de Polícia (Convenção Europol) e o Protocolo relativo aos privilégios e imunidades da Europol, dos membros dos seus órgãos, dos seus directores-adjuntos e agentes". [JO C 312 de 16/12/2002]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:312:0001:0007:PT:PDF]

_____. 2003. "Uma Europa Segura num Mundo Melhor - Estratégia Europeia em Matéria de Segurança". Disponível em:
[http://consilium.europa.eu/uedocs/cmsUpload/031208ESSIIP.pdf]

_____. 2004. “Acto do Conselho, de 27 de Novembro de 2003, que, com base no n.º 1 do artigo 43.º da Convenção que cria um Serviço Europeu de Polícia (Convenção Europol), estabelece um protocolo que altera essa convenção”. [JO C 2 de 06/01/2004]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:002:0001:0012:PT:PDF]

_____. 2005. “Decisão-Quadro 2005/222/JAI do Conselho de 24 de Fevereiro de 2005 relativa a ataques contra os sistemas de informação. [JO L 69 de 16/03/2005]”. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PT:PDF]

_____. 2009. “Actos Aprovados ao Abrigo do Título VI do Tratado UE - Decisão do Conselho de 6 de Abril de 2009 que cria o Serviço Europeu de Polícia (Europol)”. [JO L 121 de 15/05/2009]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:PT:PDF]

_____. 2010. “Estratégia de segurança interna da União Europeia – Rumo a um modelo europeu de segurança”. Secretariado-Geral do Conselho. Luxemburgo: Serviço das Publicações da União Europeia. Disponível em:
[http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313PTC.pdf]

_____. 2011a. “Europol Work Programme 2012”. [ENFOPOL 268]. Disponível em:
[http://register.consilium.europa.eu/pdf/en/11/st13/st13516.en11.pdf]

_____. 2011b. “Projecto de Conclusões do Conselho que fixam as prioridades da UE em matéria de luta contra a criminalidade organizada para o período de 2011 a 2013”. [11050/11]. Disponível em:
[http://register.consilium.europa.eu/pdf/pt/11/st11/st11050.pt11.pdf]

CONSELHO EUROPEU. 1995. “Acto do Conselho de 26 de Julho de 1995 que estatui a Convenção elaborada com base no artigo K.3 do Tratado da União Europeia que cria um serviço Europeu de Polícia (Convenção Europol)”. [JO C 316 de 27/11/95]. Disponível em:

[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1995:316:0001:0032:PT:PDF]

_____. 2008. "Relatório sobre a Execução da Estratégia Europeia de Segurança: Garantir a Segurança num Mundo em Mudança". [S407/08]. Disponível em: *[http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/PT/reports/104638.pdf]*

_____. 2010. "Programa de Estocolmo — Uma Europa Aberta e Segura que Sirva E Proteja os Cidadãos". Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:pt:PDF]*

ENISA. 2009. "Cloud Computing – Benefits, risks and recommendations for information security". Disponível em: *[http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport]*

_____. 2011a. "Cyber Europe 2010 – Evaluation Report". Disponível em: *[http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report/at_download/fullReport]*

_____. 2011b. "Proactive detection of network security incidents, report". Disponível em: *[http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report/at_download/fullReport]*

_____. 2012a. "Work Programme 2012 – Improving Information Security Through Collaboration" Versão 4.1. Disponível em: *[http://www.enisa.europa.eu/publications/programmes-reports/WP2012.pdf]*

_____. 2012b. "The Fight against Cybercrime - Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices". Disponível em: *[http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices/at_download/fullReport]*

EUROPOL. 2007. “The Strategy of Europol”. Disponível em:
[http://www.statewatch.org/news/2007/sep/Europol-strategy-12530-07.pdf].

_____. 2009. “Ten Years of Europol – 1999-2009”. Netherlands: European Police Office. Disponível em:
[https://www.Europol.europa.eu/sites/default/files/publications/anniversary-publication.pdf]

_____. 2010. “EUROPOL Review - General report on Europol Activities”. European Police Office. Disponível em:
[https://www.Europol.europa.eu/sites/default/files/publications/Europolreview2009.pdf]

_____. 2011a. “The Future of Organised Crime and Terrorism in the European Union”. European Police Chiefs Convention. Netherlands: European Police Office. Disponível em:
[https://www.Europol.europa.eu/sites/default/files/publications/epcc2011report.pdf]

_____. 2011b. “EUROPOL Review - Relatório Geral sobre as Actividades da Europol”. European Police Office. Disponível em:
[https://www.Europol.europa.eu/sites/default/files/publications/pt_Europolreview.pdf].

_____. 2011c. “iOCTA, Internet Facilitated Organised Crime”. The Hague: 07/01/11 Documento nº 2530-264. Disponível em:
[https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf]

G8/G20. 2011. “Delegations of the G8 & G20 Youth Summits – G8 & G20 Youth Summits, Paris 2011 – Final Communiqué”. Disponível em:
[http://g8-g20-youth-summits.org/FCYS.pdf]

HUI, Khoo Boon. 2011. “Remarks by Khoo Boon Hui - INTERPOL President - 80th INTERPOL General Assembly”. Disponível em:
[http://www.Interpol.int/content/download/12346/84934/version/2/file/GA80KhooOpening.pdf]

INTERPOL. 2008. “INTERPOL history”. Disponível em:
[https://www.Interpol.int/Public/ICPO/Governance/SG/History.pdf]

_____. 2011a. "ICPO-INTERPOL Constitution and General Regulations". França: Lyon, General Secretariat. Disponível em:
[http://www.Interpol.int/en/content/download/9429/69209/version/5/file/ConstitutionGene]

_____. 2011b. "INTERPOL Annual Report 2010". França: Lyon, General Secretariat. Disponível em:
[http://www.Interpol.int/content/download/8584/64691/version/11/file/Annual%20Report%202010_English.pdf]

_____. 2012a. "INTERPOL is the world's largest international police organization, with 190 member countries". Disponível em:
[http://www.Interpol.int/en/News-and-media/News-media-releases/NAbout]

_____2012b. "INTERPOL Fact Sheet - I-link: connecting investigations worldwide". Disponível em:
[http://www.Interpol.int/content/download/789/6339/version/13/file/Factsheets_EN_feb2]

_____. 2012c. "INTERPOL Fact Sheet - Connecting police: I-24/7". Disponível em:
[http://www.Interpol.int/content/download/787/6307/version/13/file/Factsheets_EN_feb2012_GI03.pdf]

_____. 2012d. "INTERPOL Fact Sheet - Databases". Disponível em:
[http://www.Interpol.int/content/download/788/6323/version/13/file/Factsheets_EN_feb2012_GI04.pdf]

_____. 2012e. "INTERPOL Fact Sheet - INTERPOL: an overview". Disponível em:
[http://www.Interpol.int/content/download/785/6275/version/14/file/Factsheets_EN_feb2012_GI01.pdf]

_____. 2012f. "INTERPOL Global Complex for Innovation" Newsletter janeiro 2012. Disponível em:
[http://www.Interpol.int/content/download/13111/91504/version/10/file/Newsletter2.pdf]

_____. 2012g. "'World must better prepare itself for emerging cybercrime threats', INTERPOL Chief tells prestigious meeting in India". INTERPOL Media Release. Disponível em:
[http://www.Interpol.int/News-and-media/News-media-releases/2012/PR028]

ITU. 2005. “A Comparative Analysis of Cybersecurity Initiatives Worldwide”. Publicação ITU. Disponível em:
[http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf]

_____. 2006. “Facilitation Meeting for WSIS Action Line C5: Building confidence and security in the use of ICTs - Chairman’s Report ‘Partnerships for Global Cybersecurity’”. Publicação ITU. Disponível em:
[http://www.itu.int/osg/csd/cybersecurity/2006/chairmansreport.pdf]

_____. 2009a. “Series X: Data Networks, Open System Communications and Security. Telecommunication security. Overview of Cybersecurity. Recommendation ITU-T X.1205”. Publicação ITU. Disponível em:
[http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items]

_____. 2009b. “Understanding Cybercrime: a guide for developing countries”. Publicação ITU. Disponível em:
[http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf]

_____. 2011a. “The world in 2011, ICT Facts and Figures”. Publicação ITU. Disponível em:
[http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf]

_____. 2011b. “ITU National Cybersecurity Strategy Guide”. Publicação ITU. Disponível em:
[http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf]

_____. 2011c. “IMPACT: International Multilateral Partnership Against Cyber Threats”. Disponível em:
[http://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT_Factsheet_FA.pdf]

NATO. 2010. “Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation”. Disponível em:
[http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf]

_____. 2011. “Cyberdefence, Key trends and Statistics”. Disponível em: *[http://www.nato.int/cps/en/SID-22BBC4AF-928A598B/natolive/photos_76221.htm]*

OCDE/ITU. 2011. “M-Government: Mobile Technologies for Responsive Governments and Connected Societies, OCDE Publicações. Disponível em: *[http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan047499.pdf]*

OCDE. 2006. “OCDE Studies in Risk Management – Norway - Information Security”. Publicações OECD. Disponível em: *[http://www.oecd.org/dataoecd/36/16/36100106.pdf]*

_____. 2007. “Computer Viruses And Other Malicious Software, A Threat To The Internet Economy”. Ministerial Background Report referência n.º DSTI/ICCP/REG(2007)5/FINAL. Disponível em: *[http://www.oecd.org/dataoecd/53/34/40724457.pdf]*

_____. 2012a. “OECD Factbook 2011-2012: Economic, Environmental and Social Statistics”. Publicações OECD. Disponível em: *[http://www.oecd-ilibrary.org/sites/factbook-2011-en/index.html;jsessionid=23tbqb0po5icc.epsilon?contentType=/ns/Book,/ns/StatisticalPublication&itemId=/content/book/factbook-2011-en&containerItemId=/content/serial/18147364&accessItemIds=&mimeType=text/html]*

_____. 2012b. “Machine-to-Machine Communications: Connecting Billions of Devices”. OECD Digital Economy Papers: n.º 192, OECD Publishing. Disponível em: *[http://dx.doi.org/10.1787/5k9gsh2gp043-en]*

ONU. 1994. “Manual on the Prevention and Control of Computer-Related Crime.” United Nations publicações, No. E.94.IV.5. Disponível em: *[http://www.uncjin.org/Documents/EighthCongress.html]*

_____. 2001a. “Carta das Nações Unidas e Estatuto da Corte Internacional de Justiça”. Rio Janeiro: Centro de Informação das Nações Unidas.

_____. 2001b. “Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)] - 55/63. Combating the criminal misuse of information technologies”. [A/RES/55/63]. Disponível em:
[http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf]

_____. 2010a. “Twelfth United Nations Congress on Crime Prevention and Criminal Justice” [A/CONF.213/9] Salvador, Brazil, 12-19 April. Disponível em:
[http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf]

_____. 2010b. “Delegates consider best response to Cybercrime as Congress Committee - Takes up dark side of advances in information technology - Subsidiary Body Divided over Whether to Expand Existing Convention or Start Negotiations on New Treaty”. [SOC/CP/349]. Disponível em:
[http://www.un.org/News/Press/docs/2010/soccp349.doc.htm]

PARLAMENTO EUROPEU. 2004. “Regulamento (CE) N.º 460/2004 do Parlamento Europeu e do Conselho de 10 de Março de 2004 que cria a Agência Europeia para a Segurança das Redes e da Informação.” [JO L 77/2004]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:PT:PDF]

_____. 2010. “Debate anual sobre os progressos realizados no Espaço Europeu de Liberdade, Segurança e Justiça (artigos 2.º e 39.º do Tratado UE) - Resolução do Parlamento Europeu, de 24 de Abril de 2009, sobre o debate anual sobre os progressos realizados em 2008 no Espaço de Liberdade, de Segurança e de Justiça (ELSJ) (artigos 2.º e 39.º do Tratado UE)”. [JO C 184 E de 08/07/2010]. Disponível em:
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:184E:0090:0094:PT:PDF]

TOURÉ, Hamadoun I. 2011. “Cybersecurity Global status update”. Apresentação ITU. Disponível em:
[http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf]

UNIÃO EUROPEIA. 1992. “Tratado da União Europeia.” [JO C 191 de 29/7/1992]. Disponível em:
[http://eur-lex.europa.eu/pt/treaties/dat/11992M/htm/11992M.html]

_____. 2010a. “Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a ataques contra os sistemas de informação e que revoga a Decisão-Quadro 2005/222/JAI do Conselho”. [COM(2010)517]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PT:PDF]*

_____. 2010b. “Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura”. [COM(2010)673]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:PT:PDF]*

_____. 2010c. “Uma Agenda Digital para a Europa” Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. [COM(2010)245/2]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PT:PDF]*

_____. 2010d. “Documento de Trabalho dos Serviços da Comissão - Resumo da Avaliação de Impacto - Documento que acompanha a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)”. [SEC(2010)1127]. Disponível em: *[http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2010/1127/COM_SEC(2010)1127_PT.pdf]*

_____. 2010e. “Communication from the Commission to the European Parliament and the Council – Overview of information management in the area of freedom, security and justice”. Disponível em: [COM(2010)385] *[http://www.statewatch.org/news/2010/jul/eu-com-overview-information-management-com-385-10.pdf]*

_____. 2010f. “Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Realização de um espaço de liberdade, de segurança e de justiça para os cidadãos europeus - Plano de Acção de aplicação do Programa de Estocolmo”. [COM(2010)171]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:PT:PDF]*

_____. 2010g. “Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of Europol’s activities by the European Parliament, together with national Parliaments”. [COM(2010)776]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0776:FIN:EN:PDF]*

_____. 2010h. “Versões Consolidadas do Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia”. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:FULL:PT:PDF]*

_____. 2011. “Realizações e próximas etapas: para uma cibersegurança mundial” Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. [COM(2011)163]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:PT:PDF]*

_____. 2012. “Comunicação da Comissão ao Conselho e ao Parlamento Europeu – Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade”. [COM(2012)140]. Disponível em: *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:PT:PDF]*

UNICRI. 2012. “Link between Organised Crime and Cybercrime”. Disponível em: *[http://www.unicri.it/emerging_crimes/cybercrime/explanations/organised_crime.php]*

UNITED STATES OF AMERICA. 2010. “National Security Strategy”. The White House, Washington. Disponível em: *[http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf]*

_____. Central Intelligence Agency. 2002. “The Questions for the Record from the Worldwide Threat Hearing on 6 February 2002.” em *The Worldwide Threat,* Senate Select Committee on Intelligence. Disponível em: *[http://www.fas.org/irp/congress/2002_hr/020602cia.html]*

_____. Department of Defense. 2010. Dictionary of Military and Associated Terms, 8 Novembro 2010. Joint Publication 1-02. Disponível em: *[http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf]*

_____. Government Accountability Office. 2010. “CYBERSPACE - United States Faces Challenges in Addressing Global Cybersecurity and Governance” United States Government Accountability Office, Report to Congressional Requesters. Disponível em: *[http://gao.gov/assets/310/308401.pdf]*

UNODC. 2005. “World Drug Report 2005”. Disponível em: *[http://www.unodc.org/pdf/WDR_2005/volume_1_web.pdf]*

_____. 2010. “The Globalization of Crime - A Transnational Organized Crime Threat Assessment”. Publicação United Nations. Disponível em: *[http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf]*

_____. 2011. “World Drug Report 2011”. Disponível em: *[http://www.unodc.org/documents/data-and-analysis/WDR2011/World_Drug_Report_2011_ebook.pdf]*

ENTREVISTAS

FONTE CONFIDENCIAL A e B DO SIS. 2012. “Entrevista exploratória n.º2”. Entrevistados pelo autor em 4 de abril de 2012. Lisboa: Forte da Ameixoeira, SIS.

MORGADO, Maria José. 2012. “Entrevista exploratória n.º3”. Entrevistados pelo autor em 19 de abril de 2012. Lisboa: DIAP.

TRIBOLET, José. 2012. “Entrevista exploratória n.º4”. Entrevista enviada via *e-mail*, respondida em 18 de março de 2012.

RODRIGUES, Benjamim Silva. 2012. “Entrevista exploratória n.º5”. Entrevista enviada via *e-mail*, respondida em 19 de março de 2012.

VERDELHO, Pedro. 2012. “Entrevista exploratória n.º6” Entrevista enviada via *e-mail*, respondida em 18 de abril de 2012.

PALMER, Adam. 2012. "Entrevista exploratória n.º7". Entrevista enviada via *e-mail*, respondida em 15 de março de 2012.

DUFKOVA, Andrea. 2012. "Entrevista exploratória n.º8". Entrevista enviada via *e-mail*, respondida em 15 de março de 2012.

TIKK, Eneken. 2012. "Entrevista exploratória n.º9". Entrevista enviada via *e-mail*, respondida em 01 de abril de 2012.

CAVELTY, Myriam Dunn. 2012. "Entrevista exploratória n.º10". Entrevista enviada via *e-mail*, respondida em 03 de abril de 2012.

FONTES SECUNDÁRIAS

ALBRIGHT, David; BRANNAN, Paul; Walrond, CHRISTINA. 2010. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Preliminary Assessment, ISIS Report. Disponível em:
[http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf]

ALVES, Armando Carlos. 2010. "Introdução à Segurança." Lisboa: Revista da Guarda.

ALVES, Flávio dos Santos Alves. 2005. "Oficiais de Ligação da PSP na Cooperação Policial Internacional", em PEREIRA, João Manuel, NEVES, Joaquim (Coord.), *Estratégia e Gestão Policial em Portugal*. Oeiras: INA.

ARQUILLA, John e RONFELDT, David Ronfeldt. 1993. "Cyberwar is Coming!" *Comparative Strategy*12 (2):141–165. Disponível em:
[http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485253]

BALÃO, Sandra Maria Rodrigues. 2010. "Geoestratégia do Ciberespaço. Contributos para uma Estratégia da Informação Nacional". *Proelium*: (13). Disponível em:
[http://www.academiamilitar.pt/proelium-n.o-13/a-geopolitica-e-geoestrategica-no-ciberespaco.html]

BARLOW, John Perry. 1996. "Declaração de Independência do Ciberespaço". Davos. Disponível em:
[http://www.dhnet.org.br/ciber/textos/barlow.htm] e *[http://editions-hache.com/essais/pdf/barlow1.pdf]*

_____. 2010. "The Power of the Internet". Alocução proferida num evento independente organizado por TEDxHAMBURG em Berlim, Alemanha, em 27 de Maio de 2010. Disponível em:
[http://www.youtube.com/watch?v=4XCg3j9jY6A&feature=player_embedded]

BERKOWITZ, Bruce; HAHN, Robert W. 2003. "Cybersecurity: Who's Watching the Store?". *Science and Tecnhology*19 (03): 55-62. Disponível em:
[http://regulation2point0.org/wp-content/uploads/downloads/2010/04/phpe4.pdf]

BORCHARDT, Klaus-Dieter. 2000. "O ABC do Direito Comunitário". Coleção *Documentação Europeia*. Trad. Comissão Europeia. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 5ª ed.
Disponível em: *[http://ec.europa.eu/publications/booklets/eu_documentation/02/txt_pt.pdf]*

BRANDÃO, Ana Paula. 2003. "Para uma política de segurança global da UE" Europa: *Novas Fronteiras*. 13/14. Centro de Informação Europeia Jacques Delors. São João do Estoril: Principia

_____. 2004. "Segurança: um conceito contestado em debate", em MOREIRA, Adriano (Coord.).2004. *Informações e Segurança. Estudos em Honra do General Pedro Cardoso*. Lisboa: Prefácio: 37-55.

_____. 2010a. "O Tratado de Lisboa e a *Security Actorness* da UE", *Relações Internacionais* 25: 49-63. Disponível em:
[http://www.scielo.oces.mctes.pt/pdf/ri/n25/n25a06.pdf]

_____ (Coord.), et al. 2010b. *A União Europeia e o terrorismo transnacional*. Coimbra: Almedina.

_____. 2011. "A Externalização da Segurança Interna: Cooperação Policial Europeia e Terrorismo Transnacional" Comunicação submetida ao XI Congresso Luso-Afro-Brasileiro de Ciências Sociais (CONLAB), Bahia, 7-11 de Agosto de 2011. Disponível em:

[http://www.xiconlab.eventos.dype.com.br/resources/anais/3/1307749227_ARQUIVO_Brandao,AP-CONLAB2011c.pdf]

CARMO, Pedro do. 2010. "Segurança dos cidadãos: a contribuição das Forças e dos Serviços de Segurança. Polícia Judiciária", em "I Jornadas de Segurança Interna. 2010. Ministério da Administração Interna" – Direção Geral de Administração Interna, Lisboa: MAI/DGAI: 151-152.

CARRAPIÇO, Helena. 2005. "O Crime Organizado e as Novas Tecnologias: uma Faca de Dois Gumes." *Revista Segurança e Defesa*: (111): 175-192.

_____. 2008. "A União Europeia e a Intelligence – Parte I". Disponível em: *[http://www.revistaautor.com/portal/index.php?view=article&catid=101%3Ainternacional&id=361%3Aa-unieuropeia-e-a-intelligence--parte-i&format=pdf&option=com_content&Itemid=49]*

CASTELLS, Manuel. 2005. *A Sociedade em Rede - A Era da Informação: economia, sociedade e cultura*. Vol 1.Tradução de Roneide Venâncio Majer. 8ª edição. São Paulo: Paz e Terra.

_____. 2005. "A Sociedade em Rede: do Conhecimento à Política." em CARDOSO, Gustavo.; CASTELLS, Manuel, *A Sociedade em Rede: do Conhecimento à Acção Política*. Lisboa: Imprensa Nacional da Casa da Moeda, p. 17-30. Disponível em: *[http://www.cies.iscte.pt/destaques/documents/Sociedade_em_Rede_CC.pdf]*

CAVELTY, Myriam Dunn. 2007. "Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology & Politics* 4(1):19-36. Disponível em: *[http://www.jitp.net/files/v004001/JITP4-1_Cyber_Terror_Cavelty.pdf]*

_____. 2009. "Cyber-threats". em MAUER, Victor e CAVELTY, Myriam Dunn (edit). "*The Routledge Handbook of Security Studies*". Londres: Routledge: 180-189.

CHEANG, Aloysius. 2009. "Guidelines for Cibersecurity". *Jornal Synthesis* (Spring): 9-16. Disponível em: *[http://www.itsc.org.sg/pdf/synthesis09/Two_Cybersecurity.pdf]*

CLEMENTE, Pedro José Lopes e FERNANDO. 2007. "Segurança e Urbanismo – O olho d'Hours". *Revista da Polícia Portuguesa*(5):.38-39.

DAVIN, João. 2007. *A Criminalidade Organizada Transnacional – A Cooperação Judiciária e Policial na UE*. Coimbra: Edições Almedina.

DECHAMP, Claude. 2005. "Cybercriminalité". *Defense Nationale*(4):99-114.

DENNING, Dorothy 2001. "Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy". em ARQUILLA, John e RONFELDT, David (edits.), *Networks and Netwars The Future of Terror, Crime, and Militancy*. RAND Corporation: parte III, capítulo 8: 239-288. Disponível em: *[http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf]*

_____. 2003. "Information Technology and Security." Versão de pré-publicação em *Grave New World*: Global Dangers in the 21stCentury. Editado por Michael Brown. Georgetown Press. Disponível em: *[http://faculty.nps.edu/dedennin/publications/IT%20and%20Security%20-%20Grave%20New%20World.pdf]*

Dicionário Editora da Língua Portuguesa 2011. Porto: Porto Editora.

DOGRUL, Murat; ASLAN, Adil; CELIK, Eyyup. 2011."Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism" em *3rd International Conference on Cyber Conflict.* NATO CCDCOE Publications: Estónia: 29-43. Disponível em: *[http://www.ccdcoe.org/publications/2011proceedings/DevelopingAnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf]*

FÄGERSTEN, Björn. 2010. "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol". *Intelligence and National Security* 25 (4): 500 –520. Disponível em: *[http://dx.doi.org/10.1080/02684527.2010.537028]*

FARINHA, Luís Manuel. 2005. "A Polícia de Segurança Pública e a Cooperação Policial", em PEREIRA, João Manuel, NEVES, Joaquim (Coord.), *Estratégia e Gestão Policial em Portugal*. Oeiras: INA.

FISHER, Eric. 2005. "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options" em *CRS Report for Congress.* Congressional Research Service: 22 de Fevereiro. Disponível em:
[http://fpc.state.gov/documents/organization/43393.pdf]

FREIXO, Manuel João Vaz. 2011. *Metodologia científica. Fundamentos, Métodos e Técnicas*. 3ªedição. Lisboa: Instituto Piaget.

GANUZA, N.; HERNÁNDEZ, A.; BENAVENTE, D. 2011. "An Introductory Study to Cyber Security in NEC". NATO CCDCOE Publications: Estónia. Disponível em:
[http://www.ccdcoe.org/articles/2011/An_Introductory_Study_to_Cyber_Security_in_NEC.pdf]

GIDDENS, Anthony. 1995. *As Consequências da Modernidade, Sociologias*. 2ª edição. Oeiras: Celta Editora. (trabalho original publicado em 1990).

Glossário de Termos Informáticos do Instituto Informático. Autoria da Comissão Técnica Portuguesa de Normalização de Terminologia Informática (CT 113). Última atualização: 2008/01/29. Disponível em:
[http://www.inst-informatica.pt/ct113/port.htm]

GOMES, Paulo Jorge Valente Gomes. 2005. A Cooperação Policial na União Europeia – Um desafio Estratégico para a PSP, em PEREIRA, João Manuel, NEVES, Joaquim (Coord.), *Estratégia e Gestão Policial em Portugal*. Oeiras: INA.

GOODMAN, Marc D.; BRENNER, Susan W. 2002. "The Emerging Consensus on Criminal Conduct in Cyberspace". *International Journal of Law and Information Technology*10 (2). Disponível em:
[http://law.scu.edu/international/File/goodmanbrenner.pdf]

GUILD Elspeth et al. 2010. *The Area of Freedom, Security and Justice Ten Years on Successes and Future Challenges Under the Stockholm Programme*. Centre for Bruxelas: European Policy Studies.

HALPERIN, Daniel et al. 2008. “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, Proceedings of the 2008 IEEE Symposium on Security and Privacy”. Disponível em:
[http://www.secure-medicine.org/icd-study/icd-study.pdf]

HERT, Paul de; FUSTER, Gloria González e KOOPS, Bert-Jaap. 2006. “Fighting Cybercrime in the Two Europes. The Added Value of the EU Framework Decision and the Council of Europe Convention”. *International Review of Penal Law* (77):503-524. Disponível em:
[http://www.vub.ac.be/LSTS/pub/Dehert/260.pdf]

HOLLIS, Duncan B. 2011. “An e-SOS for Cyberspace”. *Harvard International Law Journal*: 52(2): 373-432. Disponível em:
[http://poseidon01.ssrn.com/delivery.php?ID=271115095026085002010106011107106O]

HUTCHINSON, William. 2006. “Information Warfare and Deception“.*Informing Science*9: 213-223. Disponível em:
[http://inform.nu/Articles/Vol9/v9p213-223Hutchinson64.pdf]

JESUS, Diego Santos Vieira de. 2011. “Um discurso sobre métodos: metodologias para o estudo das Relações Internacionais na contemporaneidade.” *Revista de economia & Relações Internacionais da Faculdade de Economia da Fundação Armando Alvares Penteado*9(18): 121-137.

KIRCHNER, Emil J.; e SPERLING, James (Edit.). 2007. *Global Security Governance. Competing perceptions of security in the 21st century*. London: Routledge.

KRANZBERG, M. 1985. “The information age: evolution or revolution*”.* Citado em CASTELLS, Manuel, *A Sociedade em Rede - A Era da Informação: economia, sociedade e cultura*. 2005. Tradução de Roneide Venâncio Majer. 8ª edição. São Paulo: Paz e Terra, volume 1:113.

LÉVY, Pierre. 1997. *O que é o virtual?*. Tradução de Paulo Neves. São Paulo: Editora 34.

_____. 1999. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34.

LUSA. 2011. “Mais horas de História e Geografia nos 7º e 9º anos” *apud Diário de Notícias*: 12/12/2011. Disponível em: *[http://www.dn.pt/inicio/portugal/interior.aspx?content_id=2178876&page=-1]*

MOREIRA, Adriano. 2010. *Teoria das Relações Internacionais*. 6ª ed. Coimbra: Almedina.

NABAIS, Tiago Veloso Nabais. 2011. “Prevenção do Terrorismo Transnacional - A Partilha de Informações no Quadro da Europol” (Dissertação de Mestrado). Orientadora: Prof.ª Doutora Ana Paula Brandão. Lisboa: ISCPSI.

NUNES, Paulo Viegas. 2010. “Mundos Virtuais, Riscos Reais: Fundamentos Para a Definição de Uma Estratégia da Informação Nacional” em *I Congresso Nacional de Segurança e Defesa*. Lisboa: Diário de Bordo.

OLIVEIRA, José Ferreira de. 2006. *As Políticas de Segurança e os Modelos de Policiamento – A emergência do Policiamento de Proximidade*. Coimbra: Almedina.

OTTIS, Rain; LORENTS, Peeter. 2010. “Cyberspace: Definition and Implications”. NATO CCDCOE: Estónia. Disponível em: *[http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf]*

PAUL, Christian Paul. “Rapport au Premier Ministre. Du droit et des libertés sur l’internet. La corégulation, contribution française pour une régulation mondiale”. Disponível em: *[http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//004001056/0000.pdf]*

PINGDOM. 2012. “Internet 2011 in numbers”. Publicações Pingdom. Disponível em: *[http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/]*

POLLITT, Mark M. 1997. “CYBERTERRORISM - Fact or Fancy?” *Proceedings of the 20th National Information Systems Security Conference*, outubro. Disponível em: *[http://www.cs.georgetown.edu/~denning/infosec/pollitt.html]*

RAGIN, C. 1994. “Constructing social research: the unity and diversity of method.” 1994. Citado em JESUS, Diego Santos Vieira de. 2011. “Um discurso sobre métodos: metodologias para o estudo das Relações Internacionais na contemporaneidade.” *Revista*

*de economia & Relações Internacionais da Faculdade de Economia da Fundação Armando Alvares Penteado*9(18):126.

RAUSCHER, Karl Frederick e YASCHENKO, Valery (edit.). 2011. “Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations”. East-West Institute e Information Security Institute of Moscow State University. Disponível em: *[http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf]*

ROBINSON, Glen O.. 1999. “Regulating the Internet.”. Legal Essays. Disponível em: *[http://poseidon01.ssrn.com/delivery.php?ID=001013124122078064086109029115083110051062053034039007074008022081001098127081105064091087117064101124027044067068099120101027097125075081028&EXT=pdf]*

ROBINSON, Neil *et all*. 2012. “Feasibility study for a European Cybercrime Centre”. RAND Europe. Disponível em: *[http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf]*

RODRIGUES, Benjamim Silva. 2009. *Direito Penal Parte Especial*, Tomo I, Direito Penal Informático-Digital.” Coimbra: Coimbra Editora.

RONA, Thomas. 1976. “Weapon Systems and Information War”. Disponível em: *[http://www.dod.mil/pubs/foi/homeland_defense/missile_defense_agency/09-F-0070WeaponSystems_and_Information_War.pdf]*

SALOVEN, Matjaz et all. 2010. “Study on the status of information exchange amongst law enforcementauthorities in the context of existing EU instruments”. International Centre for Migration Policy Development e European Public Law Organization. Disponível em: *[http://ec.europa.eu/home-affairs/doc_centre/police/docs/ICMPD%20Study%20LEA%20InfoEx.pdf]*

SANTO, Paula do Espírito. 2002. “Novos poderes na era da Internet”. *Revista da Polícia Portuguesa*(133):16-20.

_____. 2010. *Introdução à Metodologia em Ciências Sociais – Génese, Fundamentos e Problemas*. Lisboa: Sílabo.

SANTOS, Paulo, BESSA, Ricardo; PIMENTEL, Carlos. 2009. "C*yberwar – O Fenómeno, a Tecnologia e os Actores*" Lisboa: FCA, Editora de Informática Lda.

SCHJOLBERG, Judge Stein e HUBBARD, Amanda M. 2005. "Harmonizing National Legal Approaches on Cybercrime". Disponível em: *[http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf]*

SCHJOLBERG, Stein e GHERNAOUTI-HÉLIE, Solange. 2011. "A Global Treaty on Cybersecurity and Cybercrime" Second Edition. Disponível em: *[http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf]*

SILVA, Amado da. 2010. "O Sector das TIC na Estratégia de Segurança Nacional" em *I Congresso Nacional de Segurança e Defesa*. Lisboa: Diário de Bordo.

SILVA, António Costa. 2007. "A Segurança Energética da Europa". *Revista Segurança e Defesa*(116): 31-72

SOFAER, Abraham D. *et all*. 2000. "A Proposal for an International Convention on Cyber Crime and Terrorism". Disponível em: *[http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf]*

SYMANTEC. 2011. "W32.Stuxnet Dossier". FALLIERE, Nicolas; MURCHU, Liam o.; CHIE; Eric (edit.). 2010. Version 1.4. Disponível em: *[http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf]*

_____. 2011a). "Symantec Internet Security Threat Report, Trends for 2010". Volume 16, Published April 2011.

_____. 2011b). "2011 Norton Cybercrime Report At a Glance –Global Data" Publicação Symantec

TAFOYA, William L. 2011. "Cyber Terror".*FBI Law Enforcement Bulletin*(Novembro).. Disponível em: *[http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror]*

THOMAS, Timothy L. 2003. "Al Qaeda and the Internet: The Danger of 'Cyberplanning.'". *The United States Army's Sénior Professional Journal Parameters* 33: . 112-23.

TIKK, Eneken, KASKA, Kadri e VIHUL, Liis. 2010. "International Cyber Incidents, Legal Considerations". NATO CCDCOE Publications: Estónia. Disponível em: *[http://www.ccdcoe.org/publications/books/legalconsiderations.pdf]*

TRIBOLET, José Manuel. 2007. Prefácio de SANTOS, Paulo et. Al. 2008. *Cyberwar – O Fenómeno, a Tecnologia e os Actores*. Lisboa: FCA, Editora de Informática Lda.

_____. 2011. "Uma visão para a Estratégia da Informação Nacional". Alocução proferida no Seminário realizado no Instituto da Defesa Nacional "Ciberespaço e Estratégia Nacional da Informação" em 21 de Setembro de 2011.

VALENTE, Manuel Monteiro Guedes. 2004. "Evolução Sócio-Jurídica da Criminalidade". Revista *Arquipélago História*2ª Série (8):.281-308. Disponível em: *[http://www.estig.ipbeja.pt/~ac_direito/Manuel_Valente_p281-307.pdf]*

_____. 2009. *Teoria Geral do Direito Policial*. Coimbra: Almedina.

VENÂNCIO, Pedro Dias. 2011. *Lei do Cibercrime, Anotada e Comentada*. Coimbra: Coimbra Editora.

VENTURA, Magda M. 2007. "O estudo de caso como modalidade de pesquisa. *Revista da Sociedade de Cardiologia do Estado do Rio de Janeiro*20(5): 383-386.

VERDELHO, Pedro. 2008. "The Effectiveness of international co-operation against cybercrime: examples of good practice" *Draft* apresentado na Economic Crime Division Directorate General of Human Rights and Legal Affairs, Strasbourg, France no âmbito do "Project on Cybercrime". Disponível em: *[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/DOC-567study4-Version7_en.PDF]*

WELLMAN, Barry. (2004). “The three ages of internet studies: ten, five and zero years ago”. *New Media & Society* 6:123-129. Disponível em: *[http://homes.chass.utoronto.ca/~wellman/publications/internet-10-5-0/wellman_threeages.pdf]*

WILLIAMS, Matthew. 2010. “Cybercrime” em Brookman *et all* (edit.). 2010. Handbook *on Crime*. Willan Publishing: Cullompton:191-212.

APÊNDICES

ÍNDICE DE APÊNDICES

Note-se que as entrevistas figuram tal e qual conforme nos foram remetidas.

APÊNDICE 1

Guião da Entrevista

APÊNDICE 1

Guião da Entrevista Exploratória

A presente entrevista enquadra-se no âmbito da realização de uma Dissertação de Mestrado que aborda a Cibersegurança no quadro da Cooperação Policial Internacional. Sob a orientação da Exma. Sr.ª Professora Doutora Ana Paula Brandão, surge esta investigação no seguimento do Mestrado Integrado de Ciências Policiais e Segurança Interna ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna proposta pelo abaixo identificado como Entrevistador.

Com este método de recolha de informação queremos salientar o vínculo qualitativo da nossa investigação. Apraz-nos, desta feita, agradecer a Vossa Excelência o contributo que queremos desde já classificar como imprescindível.

Assim, pedimos-vos que tratem as vossas respostas com a maior sinceridade e objectividade. Não olvidamos o caráter anónimo/confidencial que a sua entrevista poderá assumir por razões axiomáticas. Ao tema está inerente uma natureza interdisciplinar desde as Ciências Policiais passando pela Ciência Política e Relações Internacionais e pelo Direito Penal, até áreas do saber mais técnico e específico relacionado com as Tecnologias de Informação e Comunicação; pedimos-lhe que dê o seu sábio contributo mesmo que não se reveja com a área de saber correspondente à questão.

*Sinta-se à vontade para em qualquer altura da realização desta entrevista acrescentar sugestões, pontos de vista e opiniões de assuntos que relativos ao tema que não venham plasmados nesta entrevista.

Guião da Entrevista

Nome: Clique aqui para introduzir texto.

Cargo: Clique aqui para introduzir texto.

Entidade/Organização: Clique aqui para introduzir texto.

Data/Hora: *"Campo automático"*

Local: Clique aqui para introduzir texto.

Duração: Clique aqui para introduzir texto.

Entrevistador: *Nélson Silva (Aspirante a Oficial de Polícia), XXIV Curso de Formação de Oficiais de Polícia da Polícia de Segurança Pública, nº 2405/153561. Comando: Instituto Superior de Ciências Policiais e Segurança Interna.*

1 – No que concerne à atuação Estadual, considera o fenómeno da Cibercriminalidade como prioritário? Em que aspetos e a que nível?

Clique aqui para introduzir texto.

1.1 – Do mesmo modo, agora, relativamente à atuação Internacional considera o mesmo fenómeno prioritário? Em que aspetos e a que nível?

Clique aqui para introduzir texto.

2 – Consideramos que a Cooperação Internacional é urgente e necessária na prevenção e combate das Ciberameaças. Partilha desta nossa opinião? Porquê?

Clique aqui para introduzir texto.

3 – Quais os instrumentos e estruturas de cooperação a nível Internacional de prevenção e combate à Cibercriminalidade que considera vitais e realmente funcionais?

Clique aqui para introduzir texto.

4 – As estruturas de cooperação estão coordenadas de forma eficaz? Promove-se uma real cooperação de combate à Cibercriminalidade ou qualquer outro fenómeno criminal transnacional?

Clique aqui para introduzir texto.

5 – Considera que existe efetivamente uma Cooperação Policial Internacional no combate à Cibercriminalidade? Quais as entidades envolvidas que considera relevantes? Quais os obstáculos e progressos?

Clique aqui para introduzir texto.

6 – Acredita que existe um défice de cooperação e coordenação entre as estruturas internacionais? De que modo?

Clique aqui para introduzir texto.

7 – Existindo o anterior défice, considera que esta situação fará perigar um eficaz combate e prevenção da Cibercriminalidade? Justifique.

Clique aqui para introduzir texto.

8 - A União Europeia, enquanto ator de segurança, tem como missão providenciar e tornar efetiva a cooperação para combater o Cibercrime. De entre as várias medidas implementadas quais as que realmente promovem e efetivam a cooperação policial?

Clique aqui para introduzir texto.

9 – Considera que a EUROPOL e a INTERPOL realmente promovem a cooperação policial e partilha de informações? Quais as dificuldades e resultados positivos já alcançados nestas matérias?

Clique aqui para introduzir texto.

9.1 – Estas estruturas trazem um valor acrescentado ao combate da Cibercriminalidade? De que modo?

Clique aqui para introduzir texto.

9.2 – A um nível de aplicação prática, considera que essas estruturas têm impacto a nível da atuação nacional no combate às Ciberameaças? Fundamente.

Clique aqui para introduzir texto.

10 – Considera que se verifica o princípio da cooperação mútua em Portugal no geral? Existe cooperação entre as demais entidades com competências para prevenir e combater o Cibercrime atualmente no nosso País? Em que medida?

Clique aqui para introduzir texto.

11 – Transpondo a questão agora para o nível internacional, considera existir uma permuta de informações entre os níveis nacional e internacional? Quais os obstáculos e avanços?

Clique aqui para introduzir texto.

12 – Vários autores partilham da opinião de que quando se trata de Cibersegurança esta apenas é possível se o sistema não estiver ligado à rede, ou seja, não existirá defesa possível, se este estiver ligado à rede. Concorda com este entendimento? Justifique.

Clique aqui para introduzir texto.

13 – A constante demanda da prevenção obriga-nos a questioná-lo acerca da possibilidade da mesma. Considera ser possível a prevenção quando falamos de ameaças informáticas, em constante evolução e transmutação? Como perspetiva a prevenção deste fenómeno criminal?

Clique aqui para introduzir texto.

14 – Quais os desafios futuros que a Cibercriminalidade apresentará aos Estados em geral?

Clique aqui para introduzir texto.

14.1 – No caso do Estado Português, ainda pioneiro nestes caminhos, qual o caminho a seguir para garantir a Cibersersegurança aos seus cidadãos?

Clique aqui para introduzir texto.

15 – Caso represente um serviço ou força dessegurança ou qualquer serviço com competências de segurança nestes domínios, qual o principal contributo que esse serviço em particular pode dar em matéria de Cibersegurança?

Notas/sugestões/opiniões:

Clique aqui para introduzir texto.

Muito obrigado pelo preenchimento da presente entrevista. Caso esta entrevista revista, por qualquer motivo, caratér anónimo, garantimos-lhe que será dado o devido tratamento em função desse facto.

Agradecemos mais uma vez, e muito sinceramente, a atenção e tempo disponibilizados na realização desta entrevista.

APÊNDICE 2

Entrevista SIS

APÊNDICE 2

Entrevista Exploratória n.º2

A presente entrevista enquadra-se no âmbito da realização de uma Dissertação de Mestrado que aborda a Cibersegurança no quadro da Cooperação Policial Internacional. Sob a orientação da Exma. Sr.ª Professora Doutora Ana Paula Brandão, surge esta investigação no seguimento do Mestrado Integrado de Ciências Policiais e Segurança Interna ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna proposta pelo abaixo identificado como Entrevistador.

Com este método de recolha de informação queremos salientar o vínculo qualitativo da nossa investigação. Apraz-nos, desta feita, agradecer a Vossa Excelência o contributo que queremos desde já classificar como imprescindível.

Assim, pedimos-vos que tratem as vossas respostas com a maior sinceridade e objectividade. Não olvidamos o caráter anónimo/confidencial que a sua entrevista poderá assumir por razões axiomáticas. Ao tema está inerente uma natureza interdisciplinar desde as Ciências Policiais passando pela Ciência Política e Relações Internacionais e pelo Direito Penal, até áreas do saber mais técnico e específico relacionado com as Tecnologias de Informação e Comunicação; pedimos-lhe que dê o seu sábio contributo mesmo que não se reveja com a área de saber correspondente à questão.

*Sinta-se à vontade para em qualquer altura da realização desta entrevista acrescentar sugestões, pontos de vista e opiniões de assuntos que relativos ao tema que não venham plasmados nesta entrevista.

Guião da Entrevista

Nome: *Fonte Confidencial A e B*

Cargo: *Confidencial*

Entidade/Organização: *Serviço de Informações de Segurança*

Data/Hora: *04/04/2012*

Local: *Forte da Ameixoeira, SIS*

Duração: *01h30*

Entrevistador: *Nélson Silva (Aspirante a Oficial de Polícia), XXIV Curso de Formação de Oficiais de Polícia da Polícia de Segurança Pública, nº 2405/153561. Comando: Instituto Superior de Ciências Policiais e Segurança Interna.*

1 – No que concerne à atuação Estadual, considera o fenómeno da Cibercriminalidade como prioritário? Em que aspetos e a que nível?

1.1 – Do mesmo modo, agora, relativamente à atuação Internacional considera o mesmo fenómeno prioritário? Em que aspetos e a que nível?

---

2 – Consideramos que a Cooperação Internacional é urgente e necessária na prevenção e combate das Ciberameaças. Partilha desta nossa opinião? Porquê?

Claramenente, estamos perante ameaças transnacionais daí afigurar-se necessária a cooperação interna e internacional.

3 – Quais os instrumentos e estruturas de cooperação a nível Internacional de prevenção e combate à Cibercriminalidade que considera vitais e realmente funcionais?

Podemos afirmar que a cooperação Policial existe efetivamente, pelo menos no que concerne a serviços de informações. Quanto aos serviços de informações de segurança mantemos ou tentamos manter o maior número de relações possíveis. Quanto a esta questão apenas nos pode-mos pronunciar acerca da cooperação entre congéneres, no nosso caso, serviços de informações de segurança. Um instrumento que consideramos vitais e realmente funcionais são os CSIRT's, a nível de cooperação técnica esta existe efetivamente. A questão que aqui se levanta é que estas equipas, não olvidando que funcionam com fluidez, estas apenas interagem para fazer cessar ameaças a decorrer, ou seja, remendam, eliminam ameaças a decorrer, mesmo que para isso se faça perigar os meios de prova. Veja eles podem simplesmente cortar certa ligação, o que aqui se perderá é o meio de prova certamente.

4 – As estruturas de cooperação estão coordenadas de forma eficaz? Promove-se uma real cooperação de combate à Cibercriminalidade ou qualquer outro fenómeno criminal transnacional?

Quanto as nossos serviços, ocorre definitivamente. Cooperamos em matéria de informações de segurança com a NATO por exemplo no nível internacional. A nível nacional cooperamos com o vosso DEPIPOL.

5 – Considera que existe efetivamente uma Cooperação Policial Internacional no combate à Cibercriminalidade? Quais as entidades envolvidas que considera relevantes? Quais os obstáculos e progressos?

Quanto à cooperação policial, essa vai funcionando.

6 – Acredita que existe um défice de cooperação e coordenação entre as estruturas internacionais? De que modo?

O caminho a encetar terá de passar sempre por uma harmonização legislativa. Não havendo esta última a nível internacional o combate efetivo às ciberameaças será penoso. Devem-se extinguir os "offshores Informáticos", verdadeiros oásis à margem da lei. Veja-mos, se alguma ação minha informática for criminalizada no país onde a pretendo perpetuar, posso simplesmente criar um servidor virtual num outro país onde a mesma ação não é criminalizada e encetar "dentro da legalidade" o ilícito. Desde que do ponto de vista técnico seja possível efetuar algo, tal ação não é passível de controlo. O caráter deste tipo de ameaças é eminentemente técnico. Não que isto seja um défice de cooperação, será antes um entrave à mesma.

Outro assunto que aqui podemos apontar é o facto de serem os privados ater controlo sobre os dados, o que poderá configurar-se um entrave também.

7 – Existindo o anterior défice, considera que esta situação fará perigar um eficaz combate e prevenção da Cibercriminalidade? Justifique.

---

8 - A União Europeia, enquanto ator de segurança, tem como missão providenciar e tornar efetiva a cooperação para combater o Cibercrime. De entre as várias medidas implementadas quais as que realmente promovem e efetivam a cooperação policial?

Gabinete 24/7

9 – Considera que a EUROPOL e a INTERPOL realmente promovem a cooperação policial e partilha de informações? Quais as dificuldades e resultados positivos já alcançados nestas matérias?

9.1 – Estas estruturas trazem um valor acrescentado ao combate da Cibercriminalidade? De que modo?

9.2 – A um nível de aplicação prática, considera que essas estruturas têm impacto a nível da atuação nacional no combate às Ciberameaças? Fundamente.

---

10 – Considera que se verifica o princípio da cooperação mútua em Portugal no geral? Existe cooperação entre as demais entidades com competências para prevenir e combater o Cibercrime atualmente no nosso País? Em que medida?

---

11 – Transpondo a questão agora para o nível internacional, considera existir uma permuta de informações entre os níveis nacional e internacional? Quais os obstáculos e avanços?

---

12 – Vários autores partilham da opinião de que quando se trata de Cibersegurança esta apenas é possível se o sistema não estiver ligado à rede, ou seja, não existirá defesa possível, se este estiver ligado à rede. Concorda com este entendimento? Justifique.

---

13 – A constante demanda da prevenção obriga-nos a questioná-lo acerca da possibilidade da mesma. Considera ser possível a prevenção quando falamos de ameaças informáticas, em constante evolução e transmutação? Como perspetiva a prevenção deste fenómeno criminal?

A prevenção de ameaças, neste caso, Ciberameaças é da competência do SIS.

14 – Quais os desafios futuros que a Cibercriminalidade apresentará aos Estados em geral?

Os desafio terão de passar sempre por 3 grandes temáticas já identificadas: o Cibercrime, o ciberterrorismo e a ciberespionagem. Após estas temáticas que configuram desde já desafios o tipo de utilizador/agressor terá de ser identificado quanto ao seu intuito e terá de ser analisado o resultado da sua ação. Veja-se que as técnicas criminais associadas ao Cyber são milhares, assim sendo também as ameaças. Os dois aspetos fundamentais que aumentam a nossa preocupação é a Webiquidade e a convergência tecnológica. O primeiro traduz a ideia de a rede estar disponível e acessível em todo o lado através de ligações sem fios, este tipo de ligações é quase automático e a pessoa está na rede constantemente com uma grande variedade de informação no seu dispositivo de acesso. O segundo traduz a ideia de termos um conjunto de máquinas em uma só. Veja-se que hoje um telemóvel tem GPS, ligação à internet, máquina de filmar, máquina fotográfica, etc, num passado não muito distante esta realidade traduzia-se num conjunto de máquinas isoladas que com a evolução tecnológica se concentraram num só aparelho. Os Inputs/outputs que hoje um só aparelho disponibiliza são inúmeros, toda esta realidade potencia as ciberameaças. E este fenómeno assente em dois aspetos é real, atual e é bem como continuará a ser certamente um desafio para qualquer estado.

14.1 – No caso do Estado Português, ainda pioneiro nestes caminhos, qual o caminho a seguir para garantir a Cibersersegurança aos seus cidadãos?

---

15 – Caso represente um serviço ou força dessegurança ou qualquer serviço com competências de segurança nestes domínios, qual o principal contributo que esse serviço em particular pode dar em matéria de Cibersegurança?

Como já o dissemos é missão do SIS prevenir ameaças através da produção de informações de segurança.

Notas/sugestões/opiniões:

O agente encoberto terá de ser visto com algum cuidado. O cibercrime é como a Máfia, para se entrar e ganhar a confiança dos Cibercriminosos ter-se-á certamente de cometer ilícitos, muitas vezes roçando a figura do agente provocador. A ideia do Big Brother online poderá ser perigosa para os DLG's do cidadão previstos na CRP, esses sim, nunca poderão ser olvidados neste tipo de abordagens securitárias.

APÊNDICE 3

Entrevista a Maria José Morgado

APÊNDICE 3

Entrevista Exploratória n.º3

A presente entrevista enquadra-se no âmbito da realização de uma Dissertação de Mestrado que aborda a Cibersegurança no quadro da Cooperação Policial Internacional. Sob a orientação da Exma. Sr.ª Professora Doutora Ana Paula Brandão, surge esta investigação no seguimento do Mestrado Integrado de Ciências Policiais e Segurança Interna ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna proposta pelo abaixo identificado como Entrevistador.

Com este método de recolha de informação queremos salientar o vínculo qualitativo da nossa investigação. Apraz-nos, desta feita, agradecer a Vossa Excelência o contributo que queremos desde já classificar como imprescindível.

Assim, pedimos-vos que tratem as vossas respostas com a maior sinceridade e objectividade. Não olvidamos o caráter anónimo/confidencial que a sua entrevista poderá assumir por razões axiomáticas. Ao tema está inerente uma natureza interdisciplinar desde as Ciências Policiais passando pela Ciência Política e Relações Internacionais e pelo Direito Penal, até áreas do saber mais técnico e específico relacionado com as Tecnologias de Informação e Comunicação; pedimos-lhe que dê o seu sábio contributo mesmo que não se reveja com a área de saber correspondente à questão.

*Sinta-se à vontade para em qualquer altura da realização desta entrevista acrescentar sugestões, pontos de vista e opiniões de assuntos que relativos ao tema que não venham plasmados nesta entrevista.

Guião da Entrevista

Nome: *Procuradora Maria José Morgado*
Cargo: *Diretora*
Entidade: *DIAP de Lisboa*
Data: *30-05-2014 17:150*
Local: *DIAP - Lisboa*
Duração: *20 minutos*
Entrevistador: *Nélson Silva (Aspirante a Oficial de Polícia), XXIV Curso de Formação de Oficiais de Polícia da Polícia de Segurança Pública, nº 2405/153561. Comando: Instituto Superior de Ciências Policiais e Segurança Interna.*

1 – Neste momento da nossa investigação torna-se urgente aferir se realmente existe um clima de cooperação policial relativamente à temática "Cibersegurança", nomeadamente saber a opinião do Ministério Público (MP) relativamente a esta questão.

Em matéria de Cibercriminalidade as coisas não têm funcionado muito bem. Ao nível da Investigação Criminal não funciona nenhuma rede propriamente dita com pontos de contacto, acontece que o MP quando precisa entra em contacto com a polícia judiciária, delega competências para o efeito de investigação, no entanto ainda não houve uma adaptação áquilo que é exigível no combate à Cibercriminalidade. E depois tenho a ideia, embora que exterior dado que não faço parte da PJ, que eles estão sem capacidade de resposta por falta de recursos humanos e pela explosão deste tipo de criminalidade. Digo isto porque há demoras muito grandes nos exames periciais informáticos. Chegam a atingir anos. Tenho a impressão que o número de inspetores que existem na secção de crime informático, que é a 9ª secção da diretoria de Lisboa e Vale do Tejo, neste momento não tem capacidade suficiente para responder a todos as solicitações, veja que

é uma criminalidade que disparou, e para além da cibercriminalidade também temos a criminalidade praticada por meio da internet e através do computador em que se aplica os mesmos princípios da Lei do Cibercrime. Este facto fez disparar os pedidos junto da PJ, sendo que esta não tem capacidade de resposta compatível com as exigências. O MP ainda está numa situação pior, pois não temos peritos informáticos que possam logo no início da investigação, por exemplo, recolher imediatamente a prova digital ou qualquer prova recolhida em ambiente eletrónico. Só o DIAP de Lisboa é que tem um perito informático, de resto mais ninguém tem peritos informáticos, e este perito só consegue responder aos processos excecionalmente complexos e de criminalidade excecionalmente grave, não tendo também capacidade para responder a tudo. Trata-se de uma situação de carência de recursos humanos e tecnológicos para prevenir e combater não só a criminalidade mas também a criminalidade praticada através da internet.

1.1 – E quanto aos meios tecnológicos, são suficientes?
Os meios tecnológicos nunca são suficientes. O equipamento não será o equivalente às necessidades e o mesmo sucede com o MP, o MP não tem nem um software próprio para ler e imprimir fotogramas, por exemplo, que se trata de uma ferramenta que necessitamos muito em assaltos a bombas de gasolina, ourivesarias, multibancos, etc., estou a falar de coisas ridículas pois é equipamento tecnológico necessário para combater o crime, não temos, não temos praticamente nada.

2 – Neste ponto o estabelecimento de parcerias publico-privadas poderia ser uma solução. Concorda?
Concordo, mas que não sejam como as outras. É necessário uma coisa como deve ser, e dentro dos objetivos da prossecução do interesse público. Sendo que isso teria de ser uma iniciativa do Ministério da Justiça e da Administração Interna para as polícias.

3 – Relativamente aos pontos de contacto e transversalmente a todo o tipo de criminalidade os pontos de contacto são efetivamente o que se pretende em termos de eficácia?
A cooperação na Europa até vai funcionando. Através da EUROPOL, da rede judiciária europeia e da INTERPOL em geral.

3.1 – Esta-se a referir aos tradicionais princípios de cooperação gerais?
Exacto. A nível de cooperação Internacional podem-nos pedir dados, de fornecimento de IP's por exemplo. Funciona através dos canais tradicionais do costume mas não temos um ponto de contacto específico a nível do MP. A nível da polícia judiciária, isto existe e terão de ser eles a explicar.

4 – Exato, mas por exemplo em situações de urgência para preservação urgente de dados? Em termos de eficiência dos pontos de contacto estabelecidos na PJ? Qual a sua percepção do funcionamento destes pontos de contacto? São eficazes?
Quem trabalha com isso é a PJ, no entanto julgo que se se tratar de um crime grave isso funciona. Repare que isso é informação trocada entre os polícias e eu julgo que isso funciona. Eu penso que do lado de lá, mesmo assim, a informação é dada se for necessária pelos pontos de contacto que estão ativos. Mas como esses pontos de contacto não estão sob o MP, mas sim sob a PJ, somente esta lhe poderá dar o ponto de situação sobre isto. O que se passa do lado da PJ eu não sei. Posso-lhe é adiantar, por exemplo no caso da pornografia na internet, a troca de informação funciona e a PJ tem participado em muitas operações de combate à pornografia infantil na internet, algumas delas relatadas e registadas no site da EUROPOL e que deram origem a vários processos que estão pendentes aqui no DIAP de Lisboa. Na pornografia por exemplo na UE e na EUROPOL estes funcionam. Aliás já funcionavam quando eu estive na PJ, sai de lá em 2002, e

estavam a funcionar relativamente à pornografia infantil na internet. Agora criminalidade económico-financeira pode haver aí já maiores dificuldades porque é uma área muito mais opaca e de difícil recolha de prova. Repito que terá de questionar diretamente a PJ quanto à eficácia dessa rede, pois é uma rede cuja arquitetura é de natureza policial. Eu não sou a pessoa indicada, isso do foro policial. O MP não tem nada.

5 – Concordo. Outra questão que lhe trago é relativa à harmonia da legislação que terá de existir.
Tem que haver de facto harmonização legislativa, nesse modo é que têm havido decisões-quadro no sentido dessa mesma harmonização. Isto é necessário porque temos por exemplo critérios diferentes para a conservação de dados de outros países, o que condiciona a investigação.

6 – E quanto à cooperação judicial?
Isso temos cooperação internacional intensa para todas as áreas tanto da parte de expedição quer de receção dos pedidos. Com o apoio da Rede Judiciária Europeia, ou com o apoio da EUROJUST e também da EUROPOL temos, e relativamente ao tráfico internacional de pessoas, tido operações internacionais de buscas e detenções sincronizadas. Ainda agora tivemos uma em que o DIAP foi ponto nacional único, onde cerca de 20 e tal quilos de ouro apreendido em Espanha de lesados portugueses que é transportado pelos Espanhóis para Portugal para se fazer o reconhecimento e lhes ser entregue. E isto foi feito através de uma carta rogatória em que o DIAP foi ponto nacional único. A cooperação Internacional daquilo que eu conheço, e desde que as pessoas se empenhem, funciona. Funciona, e basta que as pessoas sejam persistentes e saiba estabelecer um contacto eficaz para o efeito, e emitir depois os efeitos devidamente fundamentados. No DIAP de Lisboa temos uma experiência boa nesta matéria. Quanto ao Cibercrime, também, e através das vias tradicionais funciona, depois aquela coisa de atuação imediata e de pontos de contacto para uma localização celular por exemplo, para a recolha imediata de uma dado para prevenir ou travar um crime que está em curso, isso está sediado nas polícias. Eu penso que se algum dia houver uma coisa dessas a PJ irá funcionar.

8 – E os pedidos tradicionais? Não considera os mesmos algo morosos? Falo do próprio sistema de cooperação, a forma como ele está arquitetado.
Aqui no DIAP de Lisboa não são assim tão morosos. Olhe, é mais fácil a cooperação internacional do que a cooperação nacional. Consigo, em geral, maior rapidez numa carta rogatória do que numa carta precatória para qualquer ponto do país. É preciso é que as pessoas tenham perfil para isso, é preciso um procurador/a à frente que saiba e conheça os pontos de contacto, e normalmente falasse com qualquer autoridade judiciária de qualquer país. Evidentemente que se temos um caso muito complexo, isso será mais demorado inevitavelmente.

9 – Tenho a impressão que a estrutura é demasiado pesada e os processos não são expeditos conforme s desejaria ou exigiria.
Não, repare que o mandado de detenção europeu funciona bem, a estrutura é leve, a assistência mútua penal na Europa funciona bem porque é de contacto direto, cada serviço ou tribunal contacta o outro diretamente e isso funciona bem. Se o caso for muito muito complexo é graduado o tempo a essa complexidade. Onde a cooperação internacional é mais burucrática e menos eficaz em termos de resposta é no Reino Unido e nos EUA. As respostas são demoradas e difíceis de obter, sempre foi assim. Na Europa, e segundo a minha experiência, eu estive 3 anos no Tribunal da Relação de Lisboa onde era responsável pela coordenação da cooperação Internacional, funcionava bem, nomeadamente os mandatos de detenção europeus onde tinha os mesmos cumpridos em 10 dias sem haver oposição do arguido, e mesmo havendo

eram cumpridos em 60 dias, e com recurso eram cumpridos em 90 dias/ 120 dias. Eu acho é que há aí um mito, porque desde que as pessoas saibam o que estão a fazer funciona bem, e se por vezes demora e funciona mal é porque os pedidos são mal feitos da nossa parte. Logo são devolvidos por irregularidades do pedido. Na Europa Continental a cooperação internacional funciona. Nós, DIAP de Lisboa temos seminários internacionais, participamos em meetings na Europa. Se tivermos aqui algum problema agarramos no telefone e ligamos para o EUROJUST, e o EUROJUST tem um representante do MP de cada país, e passa-se um vou já ver o que é que se passa, vou já tratar e as coisas mais ou menos funcionam. Agora se tiverem um pedido de quilómetro, aí as coisas podem arrastar-se um bocado. Mas se houver contactos pessoais por números telefónicos, correio eletrónico além de ser feito o pedido por escrito, aminha experiência mostra que as coisas funcionam. Em relação ao Cibercrime nós temos todos os entraves, não temos pontos de contacto sediados no MP, e não temos os meios periciais de espécie nenhuma. Nas polícias acho que funcionam, acho!

Muito obrigado pelo preenchimento da presente entrevista. Caso esta entrevista revista, por qualquer motivo, caratér anónimo, garantimos-lhe que será dado o devido tratamento em função desse facto.

Agradecemos mais uma vez, e muito sinceramente, a atenção e tempo disponibilizados na realização desta entrevista.

APÊNDICE 4

Entrevista a José Tribolet

APÊNDICE 4

Entrevista Exploratória nº4

A presente entrevista enquadra-se no âmbito da realização de uma Dissertação de Mestrado que aborda a Cibersegurança no quadro da Cooperação Policial Internacional. Sob a orientação da Exma. Sr.ª Professora Doutora Ana Paula Brandão, surge esta investigação no seguimento do Mestrado Integrado de Ciências Policiais e Segurança Interna ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna proposta pelo abaixo identificado como Entrevistador.

Com este método de recolha de informação queremos salientar o vínculo qualitativo da nossa investigação. Apraz-nos, desta feita, agradecer a Vossa Excelência o contributo que queremos desde já classificar como imprescindível.

Assim, pedimos-vos que tratem as vossas respostas com a maior sinceridade e objectividade. Não olvidamos o caráter anónimo/confidencial que a sua entrevista poderá assumir por razões axiomáticas. Ao tema está inerente uma natureza interdisciplinar desde as Ciências Policiais passando pela Ciência Política e Relações Internacionais e pelo Direito Penal, até áreas do saber mais técnico e específico relacionado com as Tecnologias de Informação e Comunicação; pedimos-lhe que dê o

Guião da Entrevista

Nome: *José Manuel Nunes Salvador Tribolet*

Cargo: *Presidente e Professor Catedrático*

Organização: *INESC e Instituto de Engenharia de Sistemas e Computadores*

Data: *18/04/2012*

Local: *Respondida via e-mail.*

Duração: ---

Entrevistador: *Nélson Silva (Aspirante a Oficial de Polícia), XXIV Curso de Formação de Oficiais de Polícia da Polícia de Segurança Pública, nº 2405/153561. Comando: Instituto Superior de Ciências Policiais e Segurança Interna.*

1 – No que concerne à atuação Estadual, considera o fenómeno da Cibercriminalidade como prioritário? Em que aspetos e a que nível?

Na situação que o país atravessa urge aumentar a eficiência do Estado e da sua forma de se relacionar com os cidadãos. Para prosseguirmos tal desafio dispomos de poucas ferramentas capazes de produzir em tempo útil os efeitos desejados na eficácia e eficiência da sociedade Portuguesa, entre elas destacam-se as Tecnologias de Informação e Comunicação (TIC). Assim sendo, as TIC desempenham cada vez mais um papel central no funcionamento da sociedade. Como qualquer infraestrutura concebida pelo Homem possuem fragilidades, as quais se criminalmente exploradas podem, pela sua abrangência, ter impactos nefastos no regular funcionamento da sociedade. Considero o combate ao crescente fenómeno da Cibercriminalidade

importante, na medida em que é fulcral proteger esta nova infraestrutura e controlar a evolução do mesmo. O principal vector de atuação deve ser a prevenção, uma vez que é aquele que pode garantir um desenvolvimento confiável da utilização das TIC. No entanto a resposta não deve ser descurada, pois facilmente o país pode ficar refém de grupos organizados que explorem a dependência dos sistemas de informação.

1.1 – Do mesmo modo, agora, relativamente à atuação Internacional considera o mesmo fenómeno prioritário? Em que aspetos e a que nível?

A cibecriminalidade é por natureza um fenómeno transfronteiriço, como tal qualquer abordagem que não seja global será limitada e com o tempo inútil. É urgente atuar em vários níveis; ao nível da indústria é necessário criar mecanismos que facilitem a cooperação entre o sector privado nacional e internacional, promovendo as empresas nacionais a estarem presentes nos principais fóruns internacionais nos aspetos de prevenção e resposta a incidentes. Ao nível do Estado é necessário garantir que os militares, as forças de segurança e os serviços de informação monitorizam e identificam as ameaças às infraestruturas criticas nacionais e que se criem mecanismos de colaboração no quadro da União Europeia, da NATO, dos PALOPs e de outros países nos quais Portugal detém interesses estratégicos.

2 – Consideramos que a Cooperação Internacional é urgente e necessária na prevenção e combate das Ciberameaças. Partilha desta nossa opinião? Porquê?

Inteiramente. Sem cooperação internacional é difícil ou até impossível lidar com as Ciberameaças. As Ciberameaças são um fenómeno globalizado, como tal requer a intervenção coordenada em países distintos, regimes jurídicos distintos e envolvendo desde o cidadão, empresas, administrações públicas e forças de defesa e segurança de vários países.

3 – Quais os instrumentos e estruturas de cooperação a nível Internacional de prevenção e combate à Cibercriminalidade que considera vitais e realmente funcionais?

Os instrumentos vitais, são aqueles que, respeitando a privacidade e proteção dos dados dos cidadãos e organizações, permitam a cooperação internacional. Existem alguns casos de sucesso na indústria através das equipas CSIRT/CERT e fóruns como o TF-CSIRT. Mas para uma resposta eficiente ao fenómeno é necessário, para além de uma estrutura de cooperação, uma coordenação nas respostas, e essa atualmente é inexistente. Algumas organizações como a UE, a ONU ou a NATO têm potencial para se posicionarem nesse campo facilitando a cooperação internacional, falta saber se têm a motivação e os meios.

4 – As estruturas de cooperação estão coordenadas de forma eficaz? Promove-se uma real cooperação de combate à Cibercriminalidade ou qualquer outro fenómeno criminal transnacional?

A Cibercrimanilidade ainda é tipicamente tratada como a maior parte dos crimes em Portugal, seguindo um processo de investigação tradicional, o que devido ao peso do nosso aparelho judicial pode dificultar uma resposta eficaz. Não me parece que exista qualquer coordenação, apenas cooperações pontuais.

5 – Considera que existe efetivamente uma Cooperação Policial Internacional no combate à Cibercriminalidade? Quais as entidades envolvidas que considera relevantes? Quais os obstáculos e progressos?

A Interpol tem esse papel, no entanto desconheço a eficácia com que o mesmo é desempenhado.

6 – Acredita que existe um défice de cooperação e coordenação entre as estruturas internacionais? De que modo?

Pelas dificuldades em controlar alguns dos crimes menos sofisticados e mais comuns, como a pirataria e o pishing bancário, acredito que ainda há muito a fazer para se atingir um nível de cooperação internacional que permita uma resposta eficaz e eficiente a estes fenómenos.

7 – Existindo o anterior défice, considera que esta situação fará perigar um eficaz combate e prevenção da Cibercriminalidade? Justifique.

A cooperação é essencial para a resposta e combate à Cibercriminalidade e desempenha um papel importante na prevenção, no entanto neste último aspeto a educação e a formação são bem mais relevantes.

8 - A União Europeia, enquanto ator de segurança, tem como missão providenciar e tornar efetiva a cooperação para combater o Cibercrime. De entre as várias medidas implementadas quais as que realmente promovem e efetivam a cooperação policial?

A UE tem através das recentes linhas nos programas de incentivo à investigação e desenvolvimento (FP7) específicas para a área da cibersegurança dado passos importantes no sentido de combater o Cibercrime, nomeadamente desenvolvendo capacidades neste âmbito. Espero num futuro próximo ver a Europol a desempenhar um papel mais ativo e permitir a cooperação.

9 – Considera que a EUROPOL e a INTERPOL realmente promovem a cooperação policial e partilha de informações? Quais as dificuldades e resultados positivos já alcançados nestas matérias?

9.1 – Estas estruturas trazem um valor acrescentado ao combate da Cibercriminalidade? De que modo?

Certamente que sim, são estruturas que podem vir a desempenhar papéis extremamente importantes na prevenção e investigação do Cibercrime, nomeadamente permitindo a troca de informação sobre ameaças, coordenando com os órgãos nacionais de policia e investigação para uma atempada preservação das provas.

9.2 – A um nível de aplicação prática, considera que essas estruturas têm impacto a nível da atuação nacional no combate às Ciberameaças? Fundamente.

---

10 – Considera que se verifica o princípio da cooperação mútua em Portugal no geral? Existe cooperação entre as demais entidades com competências para prevenir e combater o Cibercrime atualmente no nosso País? Em que medida?

Infelizmente acho que apenas agora estamos a acordar para o assunto, a cooperação é escassa quer entre policias, forças armadas e indústria. Há que não esquecer que a indústria é o maior detentor dos alvos do cibercrime, bem como dos meios utilizados para o praticar, o seu envolvimento é crucial.

11 – Transpondo a questão agora para o nível internacional, considera existir uma permuta de informações entre os níveis nacional e internacional? Quais os obstáculos e avanços?

O cenário internacional não é particularmente melhor que o Português. Existem movimentações recentes por parte da NATO para definir quadros de cooperação transnacional que envolvam a indústria e os militares, esperemos poder ver resultados em breve.

12 – Vários autores partilham da opinião de que quando se trata de Cibersegurança esta apenas é possível se o sistema não estiver ligado à rede, ou seja, não existirá defesa possível, se este estiver ligado à rede. Concorda com este entendimento? Justifique.

Até finais da década de noventa, o modelo de segurança que vigorava na indústria era o da Fortaleza da Informação, no qual a informação se encontrava resguardada do exterior das organizações através de um sistema de controlo de acesso (firewall) que impedia a saída

indesejada de informação e o acesso ilegítimo à informação por parte de uma entidade externa. Este conceito levado ao extremo significaria que a segurança máxima se alcançava desligando o sistema da rede. Sendo um modelo fácil de entender, pela analogia com as fortificações que historicamente foram utilizadas para defender populações de invasores, foi rapidamente adaptado na sua versão extrema principalmente pelas forças militares e de segurança. Edificaram-se redes fechadas para tratar que deveria estar separada, chegando-se na Europa ao limite de, atualmente ainda em vários países, alguns militares terem em cima da mesa 4 PCs ligados a 4 redes distintas (rede nacional, rede Europeia, rede NATO e Internet).

No final da década de 90 e inicio do séc. XXI a indústria apercebeu-se que o modelo Fortaleza da Informação não lidava corretamente com as ameaças, era desadequada do ambiente de cooperação que se pretendia impulsionar com a adopção das novas tecnologias de comunicação, não lidava com a ameaça interna e deixava os sistemas completamente expostos uma vez ultrapassado o perímetro de segurança. No mundo da defesa o ponto de viragem foi em 2008 após uma séria intrusão na rede fechada do Pentágono, provocada por malware instalado numa Pen drive USB encontrada por um soldado americano num parque de estacionamento no Médio Oriente. Em 2010 o mediático caso do Stuxnet que teve como alvo danificar o processo de enriquecimento de urânio no Irão, demonstrou que era possível não só atacar redes fechadas, mas causar sérios danos materiais com ataques perfeitamente direcionados.

Na minha opinião, tal como existe sempre um ataque, mesmo para sistemas em redes fechadas, existem também sempre possíveis defesas. A segurança, através da implementação de múltiplos controlos, deve ser desenhada partindo do principio que os controlos vão falhar, e dependendo da criticidade da informação ou serviço a proteger devem introduzir-se camadas de controlos e mecanismos de monitorização da eficácia desses controlos (Segurança em Profundidade) e serem constantemente auditados face à sua eficácia.

Uma outra questão prende-se com a capacidade de preservação de capital informacional vital para a vida social e como Nação. A preservação de repositórios de altissima segurança – não operacionais, máximamente isolados – com potencial de reposição em caso calamidades públicas, entre as quais se conta a concretização de um ciberataque massivo e destruidor de informação operacional vital – é uma questão de bom senso. E que urge concretizar.

13 – A constante demanda da prevenção obriga-nos a questioná-lo acerca da possibilidade da mesma. Considera ser possível a prevenção quando falamos de ameaças informáticas, em constante evolução e transmutação? Como perspetiva a prevenção deste fenómeno criminal?

Mais do que possível, a prevenção é essencial para controlar o crescimento deste fenómeno. Sendo que "uma corrente é tão forte quanto o mais fraco dos seus elos" há que investir na proteção do elo mais fraco, o qual sem qualquer margem para duvidas é o fator Humano. As TIC enquanto

omnipresentes na sociedade, são extremamente recentes, as pessoas em todos os papéis que desempenham na sociedade, ainda estão longe de tomar consciência dos perigos da incorreta utilização desta ferramenta tão poderosa. A vasta maioria dos decisores políticos, dos oficiais de topo das forças armadas e de segurança, dos executivos de topo das empresas ainda não têm consciência do risco da utilização destas novas ferramentas. Tal como a generalidade da sociedade, mesmo as camadas mais jovens que vivem imersos nas novas tecnologias, não têm consciência que menosprezar a segurança dos sistemas que utilizam, poderá num futuro não muito distante colocar em risco a sua própria segurança. A cibersegurança ainda hoje é em muito vista como um problema dos engenheiros, mas no entanto é um problema que os engenheiros não conseguem resolver sozinhos.

Na minha opinião a prevenção deve acontecer principalmente por via da formação e educação de todos os agentes envolvidos, para que compreendam o fenómeno e que tal compreensão os guie nas ações quotidianas, a criação de uma cultura de cibersegurança será tão essencial para o futuro, como hoje é ensinar uma criança a atravessar uma estrada. Existe ainda muito investimento a fazer em investigação e constante desenvolvimento de soluções mais seguras. Por fim, mas não menos importante, é necessário assegurar que quem desenvolve um sistema ou solução tem a formação e qualificações necessárias para que, independentemente das pressões colocadas pelo lado dos custos e prazos, possa realizar esse trabalho de forma responsável, ética e profissional, salvaguardando a segurança dos cidadãos. Este papel cabe em muitas áreas das engenharias às ordens profissionais, também neste aspeto urge regular.

14 – Quais os desafios futuros que a Cibercriminalidade apresentará aos Estados em geral?

Nada leva a crer que o ritmo de crescimento tanto do número de ataques como da sua sofisticação venha a diminuir num futuro próximo. Acredito que vamos ver num futuro bem próximo o aumento do número de ataques dirigidos a infraestruturas concretas, bem como o aumento da utilização da componente Ciber quer pelo crime organizado, quer por organizações terroristas, quer por empresas. Em traços gerais os desafios que se colocam aos estados são os de aumentar a segurança das suas infraestruturas, com especial atenção nas chamadas infraestruturas criticas, aumentar a capacidade de responder a incidentes, de investigar cibercrimes e de desenvolver capacidades de ciberinteligência. Nos próximos anos devem desenvolver-se esforços concretos por criar uma cultura de cibersegurança nas sociedades.

14.1 – No caso do Estado Português, ainda pioneiro nestes caminhos, qual o caminho a seguir para garantir a Cibersersegurança aos seus cidadãos?

O Estado Português necessita rapidamente de enfrentar os desafios de extrema exigência do ponto de vista de cooperação. Necessita não só de introduzir uma aproximação holística na forma como

o tema é tratado na Administração Publica, mas acima de tudo, iniciar o desenvolvimento de mecanismos nacionais e internacionais de cooperação entre os principais stakeholders. Só uma abordagem global permitirá lidar com um tema que, não reconhece fronteiras ou jurisdições, num mundo onde a interdependência entre os cidadãos, os sistemas e as organizações é inegavelmente crescente e globalizada. É necessário conhecer a situação atual dos sistemas e o risco a que Portugal está exposto, é necessário criar mecanismos de cooperação entre as entidades publicas e privadas, regulamentando inclusive a obrigatoriedade de em alguns sectores declarar os incidentes que ocorram. Num período de extrema contenção financeira, urge aproveitar os fundos comunitários disponíveis para estas áreas, para promover a investigação e desenvolvimento Nacional, para que exista em Portugal know-how especializado para lidar com as ciberameaças. Não menos importante é a criação de mecanismos para responder a crises provocadas por ciberincidentes de forma eficaz e coordenada. Por fim investir também em Portugal na criação de uma cultura de cibersegurança.

15 – Caso represente um serviço ou força dessegurança ou qualquer serviço com competências de segurança nestes domínios, qual o principal contributo que esse serviço em particular pode dar em matéria de Cibersegurança?

N/A

Notas/sugestões/opiniões:

A pergunta 12 deste questionário revela uma visão arquitetonica das TICs subjacente à problematica da Cibersegurança que é, na minha opinião, deficiente.

Na verdade, a questão levantada evidencia preocupação com redes e sistemas, não relevando a dimensão informação, de forma independente, nem a dimensão "processos" isto é, fluxos de encaminhamento e decisão.

Outro dos aspectos não considerados são os que têm a ver com a identificação e capacitação dos agentes (vulgo, embora incorrecto, Identity Management) e os relacionados com monitorização (os logs) e os mecanismos de controlo activo.

A Cibersegurança, do ponto de vista exclusivamente técnico, é multidimensional, e as politicas respectivas devem ser diferenciadas consoante as diferentes dimensões, envolvendo níveis e agentes diversificados e distintos.

Muito obrigado pelo preenchimento da presente entrevista. Caso esta entrevista revista, por qualquer motivo, caratér anónimo, garantimos-lhe que será dado o devido tratamento em função desse facto.

Agradecemos mais uma vez, e muito sinceramente, a atenção e tempo disponibilizados na realização desta entrevista.

§

APÊNDICE 5

Entrevista a Benjamim Silva Rodrigues

APÊNDICE 5

Entrevista Exploratória nº5

A presente entrevista enquadra-se no âmbito da realização de uma Dissertação de Mestrado que aborda a Cibersegurança no quadro da Cooperação Policial Internacional. Sob a orientação da Exma. Sr.ª Professora Doutora Ana Paula Brandão, surge esta investigação no seguimento do Mestrado Integrado de Ciências Policiais e Segurança Interna ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna proposta pelo abaixo identificado como Entrevistador.

Com este método de recolha de informação queremos salientar o vínculo qualitativo da nossa investigação. Apraz-nos, desta feita, agradecer a Vossa Excelência o contributo que queremos desde já classificar como imprescindível.

Assim, pedimos-vos que tratem as vossas respostas com a maior sinceridade e objectividade. Não olvidamos o caráter anónimo/confidencial que a sua entrevista poderá assumir por razões axiomáticas. Ao tema está inerente uma natureza interdisciplinar desde as Ciências Policiais passando pela Ciência Política e Relações Internacionais e pelo Direito Penal, até áreas do saber mais técnico e específico relacionado com as Tecnologias de Informação e Comunicação; pedimos-lhe que dê o seu sábio contributo mesmo que não se reveja com a área de saber correspondente à questão.

*Sinta-se à vontade para em qualquer altura da realização desta entrevista acrescentar sugestões, pontos de vista e opiniões de assuntos que relativos ao tema que não venham plasmados nesta entrevista.

Guião da Entrevista

Nome: *Benjamim Silva Rodrigues*

Cargo: *Assistente*

Organização: *Instituto Superior de Contabilidade e Administração de Coimbra – Business School*

Data: *19/03/2012*

Local: *Respondida via e-mail.*

Duração: ---

Entrevistador: *Nélson Silva (Aspirante a Oficial de Polícia), XXIV Curso de Formação de Oficiais de Polícia da Polícia de Segurança Pública, nº 2405/153561. Comando: Instituto Superior de Ciências Policiais e Segurança Interna.*

1 – No que concerne à atuação Estadual, considera o fenómeno da Cibercriminalidade como prioritário? Em que aspetos e a que nível?

O fenómeno da cibercriminalidade, pelas suas características e altas "cifras negras", surge (ou deveria surgir) como uma prioridade máxima de qualquer moderno Estado de Direito Democrático. Na verdade, são milhões e milhões de euros que são sonegados, às vezes de forma imperceptível, em contas bancárias ou serviços electrónicos de

pagamento à distância, mediante técnica "de salame" ou à "guisa de furto de formigueiro". Note-se, aliás, que, estranhamente, o nosso país esqueceu a necessidade de implementar "medidas de segurança ou cibersegurança", sendo o programa "e-escolas", com fornecimento "selvagem" de material e acesso à internet um dos momentos de menor lucidez. Estão por contabilizar os atentados à honra, à imagem, o "cyberstalking" – note-se que na nossa obra Direito Penal Informático-Digital, de 2009, já alertávamos para isto e avançamos com um projecto de lei –. Depois, todos os bancos portugueses escondem que foram alvo de "cyber-ataques". Mais, os custos de apetrechamos das nossas polícias ("cyber-clops") seria fortemente contrabalançado com proveitos e poupanças económicas enormes. O Estado português está longe de ser exemplar em práticas de "cyber-segurança". Partilhamos, por isso, da opinião de que é preciso, na formação dos actores forenses e demais instâncias formais de controlo (órgãos de polícia criminal), introduzir a disciplina do Direito Penal Informático-Digital, já para não falarmos noutras ciências que permitirão uma compreensão global da realidade e um melhor combate à criminalidade (nesse sentido, veja-se o auxílio do "direito penal bioético" e/ou "genético").

1.1 – Do mesmo modo, agora, relativamente à atuação Internacional considera o mesmo fenómeno prioritário? Em que aspetos e a que nível?

As instâncias internacionais – OCDE, Conselho da Europa, Nações Unidas, G8, etc., ITU, etc. – têm vindo a acentuar a ideia de que a posse de tecnologia informática é imprescindível a um certo grau de desenvolvimento. Todavia, tal desenvolvimento não pode ser feito pela via fácil da aquisição da tecnologia, já que se afigura imprescindível "educar para a tecnologia" e, sobretudo, implementar fortes medidas de segurança e códigos de conduta férreos, sob pena de o "ciberespaço" se tornar numa "zona de não-direito", onde a ilusão de impunidade inspiraria os mais atrozes crimes. Não se esqueça que podem ser cometidos crimes transnacionais e, com um simples clique, se pode desligar o sistema de suporte de vida de um hospital ou inocular e introduzir, num sistema de ar condicionado, um vírus. As redes de informação e comunicação à distância e as redes informáticas publicamente acessíveis são tão importantes, no dealbar do século XXI, como o são ou o foram, outrora, a água, a roda, etc. O ciberespaço e o "permanente refazer" de tal espaço, pelas populações, gera, simultaneamente, atractividade e preocupações. O "cyber-crime", o "crime informático", o "crime informático-digital", os ataques aos sistemas de informação, o recurso às novas tecnologias para cometimento de crimes clássicos é uma realidade. Todos os crimes clássicos podem ganhar com uma investigação "informático-digital". Basta pensar que no computador do que foi alvo de um homicídio pode estar uma ameaça do autor de tal crime, etc. A

tecnologia adquire-se facilmente, basta ter dinheiro. Estranhamente, "en brûlant les étapes", até os países "emergentes" possuem dinheiro para adquirir tecnologia, mas o mais difícil é manter os adequados níveis de "ciber"-segurança.

2 – Consideramos que a Cooperação Internacional é urgente e necessária na prevenção e combate das Ciberameaças. Partilha desta nossa opinião? Porquê?

A natureza e características da criminalidade "informático-digital" impelem, irremediavelmente, para níveis adequados de cooperação. Com a Convenção de Budapeste – 2001 – os países europeus deram um grande passo. Passo esse tão grande que até outros países, que não membros do Conselho da Europa, acharam por bem aderir a tal instrumento. Há, ainda, depois de tal instrumento, outros instrumentos internacionais que visam implementar níveis mais profundos de cooperação internacional. Entre nós, e já para não aludir à Convenção de Haia (dos Tratados), a Lei n.º 144/99, de 31 de Agosto, já possuía mecanismos mínimos – como já expusemos no nosso Direito Penal Informático-Digital (2009) – que, todavia, padeciam de "estreiteza de olhar". Os tempos são outros. O carácter global, trans-nacional e plurilocalizado ou multi-organizado do cibercrime exigem níveis adequados de cooperação internacional, sob pena de se perder na "bruma dos electrões" qualquer possibilidade de sucesso em tal tipo de combate à criminalidade informático-digital.

3 – Quais os instrumentos e estruturas de cooperação a nível Internacional de prevenção e combate à Cibercriminalidade que considera vitais e realmente funcionais?

Actualmente, julgo bastante oportuno as Redes 24/24 ou 7/7, ou seja, todos os dias da semana, durante vinte e quatro horas, os países têm operacionais que são contactáveis e têm formas expeditas de enviar, solicitar e receber informações preciosas para o combate à cibercriminalidade. A formação para a "cidadania electrónica" é uma tarefa não levada a cabo. Mais do que fornecer tecnologia gratuita é preciso ensinar, em termos cívicos, o modo de a usar. Num Estado de Direito pautado por um padrão ético-social mais elevado, como o é o português, não pode alhear-se da tarefa de colocar níveis de restrição ou precaução, ao nível das "escolhinhas", no uso e acesso à internet. Os níveis de controlo parental são importantes. Em suma, autoridades permanentemente contactáveis e cidadãos permanentemente educados para a cidadania electrónica e "privacidade electrónica", serão, de certo, mais-valias, que aumentarão o sucesso do uso das TIC e, ainda, os níveis de aproveitamento das riquezas criadas ou empoladas pelos vários sistemas de informação à distância e sistemas informático-digitais.

4 – As estruturas de cooperação estão coordenadas de forma eficaz? Promove-se uma real cooperação de combate à Cibercriminalidade ou qualquer outro fenómeno criminal transnacional?

Para responder cabalmente a esta pergunta – em perfeita honestidade intelectual – seria imprescindível que me encontrasse a colaborar directamente com alguma estrutura de cooperação. Todavia, sem prejuízo disso, dos conhecimentos e investigações que me foram dadas a levar a cabo, verifico que temos níveis de adequação e operatividade ao nível das nossas estruturas de cooperação, quer através da polícia judiciária, interpol, Rede 24/24 (representante português). O problema da cooperação internacional está sempre dependente da "benesse" do Estado demandado. Ora, como nós sabemos – e basta olhar o artigo 33.º, n.º 1, da CRP 1976 – os nacionais agarram-se (ou tendem a agarrar-se) à "saia da mãe-pátria". Esta constatação pode levar a níveis de inoperacionalidade. Um outro factor inegável é o de que nem tudo o que é "cibercrime" ou "crime", num dado país, ou é no outro e, por isso, à partida, tolhe qualquer possibilidade de sucesso.

5 – Considera que existe efetivamente uma Cooperação Policial Internacional no combate à Cibercriminalidade? Quais as entidades envolvidas que considera relevantes? Quais os obstáculos e progressos?

No dealbar do século XXI, após o lastro de convenções e instrumentos internacionais, bi-e-multilaterais, em matéria de "cibercriminalidade", não podemos negar que o "pano de fundo jurídico" já existe. Há organismos nas várias organizações internacionais – veja-se o elenco que deixamos exposto no nosso Direito Informátic-Digital (2009) – que cumprem os desideratos de uma efectiva cooperação policial internacional. As polícias dos vários Estados já reúnem e, nalguns casos, mantém mesmo sistemas "on-line" de vigilância. Matéria essa que, entre nós, como é sabido, se afigura proibida por razões constitucionalmente impostas – artigo 34.º, n.os 1 e 4, da CR$P 1976. A tutela dos dados de carácter pessoal é, ainda, um forte obstáculo à transmigração de dados e fluxos informacionais e comunicacionais que são imprescindíveis para a investigação da prova digital. Entre nós, tem vindo a discutir-se se, além da polícia judiciária, outras polícias (como a PSP) poderiam ou deveriam investigar o cibercrime. O certo é que o actual enquadramento legislativo – contrariamente ao que alguns, de modo ligeiro, propalam – não o permite, havendo um exclusivo a cargo da polícia judiciária. Não sou contra a criação de "super-polícias informático-digitais", mesmo na PSP, mas só se isso for feito em termos de correcta formação dos agentes e com competente apetrechamento técnico e com um estabelecimento de uma "cúpula de comando" comum entre esta última e

aqueloutra força policial, sob pena de ser contraproducente, como acontece várias vezes, em que as "coutadas de competências" são avessas a adequados níveis de eficácia.

6 – Acredita que existe um défice de cooperação e coordenação entre as estruturas internacionais? De que modo?

Com a ressalva que já acima formulei, pronuncio-me em termos académicos e da minha experiência de investigação nesta área, sem conhecimento directo – mas sim indirecto – de tal tema. Não julgo que exista, hoje em dia, tal défice, já que foram criadas redes de 24/24 e 7/7, com mecanismos expeditos de contacto. Reconheço que, entre nós, até por alguns modelos de investigação forense digital – reporto-me ao que é praticado pela PSP e DIAPs Lisboa – que me foram dados a conhecer, que há um longo caminho a fazer. De facto, confunde-se o que é inconfundível. Andam todos a discutir se o e-mail impresso é prova da existência da comunicação electrónica. Naturalmente, tal folha de papel vale zero e não prova sequer a existência de uma comunicação. O que prova é a prova digital, ou seja, a identificação de uma máquina informática, uma rede, um fluxo informacional e comunicacional, um emissor, um receptor, um conjunto de fornecedores de serviço de acesso à internet, etc. Sem isso nada feito. Depois, esquece-se a "chain of custody". Nalguns países, há um magistrado a selar e certificar todo o processo de recolha de prova. Entre nós, "aligeiradamente", há agentes que "fumam" nos locais de investigação, colam impressões digitais, desligam computadores, etc, etc. E, mais grave ainda, julgam-se depois "testemunhas privilegiadas" e "peritos forenses digitais". Ora tudo isto está errado e deve mudar rapidamente (e esperançosamente) com as novas gerações.

7 – Existindo o anterior défice, considera que esta situação fará perigar um eficaz combate e prevenção da Cibercriminalidade? Justifique.

Não temos qualquer dúvida de que sem cooperação (internacional) jamais poderemos falar em combate à cibercriminalidade ou, dito de outro jeito não menos próprio, será mutilante e ilusório pretender encetar tais objectivos. Se A, na Suíça, usar a rede de comunicações desse país e, depois, fizer passar o seu fluxo informacional por um "paraíso electrónico", branqueando o seu endereço IP, como será possível saber se foi aquele ataque que, no hospital de Lisboa, enviou um vírus informático que desligou a máquina de suporte de vida de um espião russo que se encontrava internado após ter sido envenenado com uma substância radioactiva? A cooperação internacional é co-natural e estruturante da cibercriminalidade, já que ela é, aparentemente, a-temporal, a-espacial, etc. O ciberespaço dá, ao mesmo tempo, a ilusão de um tempo sem espaço e um espaço sem tempo.

8 - A União Europeia, enquanto ator de segurança, tem como missão providenciar e tornar efetiva a cooperação para combater o Cibercrime. De entre as várias medidas implementadas quais as que realmente promovem e efetivam a cooperação policial?

No seio da União Europeia, no seguimento da Convenção da Cibercriminalidade (e não do Cibercrime – como erradamente foi traduzida entre nós já que são realidades distintas…), de 2001, foram implementadas várias decisões-quadro e directivas (contra os ataques aos sistemas de informação, retenção de dados) que, sem sombra de dúvidas, surgem como um lastro ou acervo legislativo apto a propiciar as condições efectivas de combate. Julgo que o estabelecimento de pontos de contacto, entre as várias forças policiais europeias, é a maior mais-valia. Depois, há que contar com outros esquemas processuais expeditos, como é o caso do mandado de detenção europeu, entre outros. Note-se que existem, depois, várias entidades que regulam a internet – veja-se o que se escreveu na obra citada e, ainda, no Tomo III Prova Penal 2011 –, os tais "actores da internet", com códigos de conduta que são, a meu ver, uma forma preventiva e proactiva de evitação de comportamentos criminosos. Depois, saliente-se que as modernas "redes sociais" já têm um exigente código de conduta e, recentemente, fala-se mesmo na obrigatoriedade de, cessando a participação de um "associado", apagarem todos os dados. Ora, este é um desafio titânico, já que a internet tem uma memória de "dinossauro", tem tendência a não esquecer o que já esqueci e vivi outrora. Entre nós, sublinhe-se, são parcas e poucas – e pobres… (académica e intelectualmente falando – como todo o respeito, obviamente, pelas entidades visadas) – as iniciativas com um nível adequado e apto a fomentar níveis de cooperação policial. Não se esquece que é preciso que o "decisor político" esteja atento. Não está. Está atento a políticas de "baixa intensidade", não se esqueça que demoramos oito anos (uma eternidade ou século no "tempo informático") para transpor a Convenção da Cibercriminalidade!

9 – Considera que a EUROPOL e a INTERPOL realmente promovem a cooperação policial e partilha de informações? Quais as dificuldades e resultados positivos já alcançados nestas matérias?

A ideia que me é transmitida – não de forma directa, sublinhe-se – é a de que esses dois organismos têm vindo a levar a cabo um trabalho não desprezível e bem coordenado. Não esqueçamos que, em Espanha, há não muito tempo, foram presos vários cibernautas. Recentemente, alguns cibernautas que provocaram a divulgação de dados privados também foram alvo de operações de tais organismos, com pleno sucesso. No caso português, o principal dilema é a ausência de consciência e vontade política. Repare-se que os nossos políticos não conseguem imaginar as perdas económicas desta

"insegurança informática". Se disso tivéssemos dúvidas, veja-se a recente operação em redor de um grupo, ligado aos medicamentos, em que se falsificaram concursos e, quiçá, empresas portuguesas foram preteridas e arcaram com perdas económicas já que cibernautas criminosos iam tendo informação privilegiada, sensível e íntima. Estou convicto que a criação de um núcleo forte, entre os vários órgãos de polícia criminal – PSP, GNR, PJ, Polícia marítima, polícia militar, ASAE, polícia municipal –, seria um bom passo e viria a contribuir para a criação de sinergia que, a julgar por alguns dados, inexistem actualmente. Tudo o que se traduzir em aumento de forças policiais e adequado material de investigação forense digital é, para mim, bem vindo e será, em rigor e no limite, um excelente instrumento de poupança ou aumento do PIB português.

9.1 – Estas estruturas trazem um valor acrescentado ao combate da Cibercriminalidade? De que modo?

A experiência da EUROPOL e INTERPOL é, sem sombras de dúvidas, uma mais-valia. De facto, os canais já estabelecidos entre ambos conseguem encurtar ou cortar barreiras que a criação de outros mecanismos, fora destes, pode não conseguir ultrapassar. Todavia, sempre direi de que nada valerão esses organismos se, entretanto, os Estados, reciprocamente, forem "esvaziando" as áreas de actuação de cada um deles, já que a não criminalização harmónica das várias matérias surge, isso sim, como um forte obstáculo. A cooperação cessa, nalguns países, por os mesmos serem demandos relativamente a condutas que consideram não serem crime.

9.2 – A um nível de aplicação prática, considera que essas estruturas têm impacto a nível da atuação nacional no combate às Ciberameaças? Fundamente.

Ninguém vive só. No mundo da cibercriminalidade, julgar possível o seu combate, policial e judicial, sem cooperação é mutilante e ilusório. As "ciberameaças" somente pode ser combatidas, pelas autoridades portuguesas, mediante adequados níveis de eficiência e cooperação com aqueles organismos internacionais. Note-se que tais organismos possuem métodos e formas de obter a informação – pelas suas redes de representantes – que o Estado português, por si só, não tem e, aliás, seria demasiado custoso e não compensador implementar.

10 – Considera que se verifica o princípio da cooperação mútua em Portugal no geral? Existe cooperação entre as demais entidades com competências para prevenir e combater o Cibercrime atualmente no nosso País? Em que medida?

Alguns episódios recentes têm vindo a colocar-nos de sobreaviso sobre a efectiva existência de cooperação, policial e judicial, mútua, quer ao nível da cibercriminalidade,

quer ao nível da demais criminalidade. Seja como for, cabe ao Estado português, mormente mediante as suas estruturas diplomáticas, implementar, bilateral ou multilateralmente, níveis adequados de cooperação. Não podemos ficar à espera de que – como sempre é hábito entre nós – os outros tudo façam por nós. Aliás, estamos convictos que, no nosso país, junto das Universidades e Politécnicos, onde se ministram cursos ligados às TIC, bem como junto de algumas empresas de sucesso, seria possível criar "clínicas informáticas" em que se estudariam as vulnerabilidades dos sistemas e se adiantariam novas soluções ou paliativos. E, frise-se, talvez com um custo reduzido. Seria interessante para os académicos. Seria desafiador para os empresários. Falta diálogo para lá da prevenção ou investigação criminal. Não houve, não há, entre nós, qualquer iniciativa, digna desse novo, com mobilização do mundo académico ou empresarial, em redor da cibersegurança como factor de crescimento industrial e económico. Nada se faz. Tudo se combate após o "derrame do leite". Também neste tipo de criminalidade é preciso "chorar antes de doer", ou seja, prevenir antes de ter de agir após um aigir jurídico-penalmente relevante e censurável.

11 – Transpondo a questão agora para o nível internacional, considera existir uma permuta de informações entre os níveis nacional e internacional? Quais os obstáculos e avanços?

Os fluxos transfronteiriços de dados informacionais ou comunicacionais, digitais ou informático-digitais, deparam – como já o referi – com uma inarredável e inabdicável tutela da reserva da vida privada. Não vale tudo na investigação criminal. A privacidade e intimidade, em geral, ou, em particular, "electrónica", são bens imprescindíveis, nos dias de hoje, já que os computadores são os novos "diários", os computadores são os novos "psicólogos", pois o ciberasto leva ao "profiling", etc. Ciente disto, há que lograr um equilíbrio. São várias as convenções e tratados nesse sentido. Note-se que, por vezes, um Estado não envia dados, importantes para a investigação, porque não tem garantias da sua protecção e, sobretudo, como temos vindo a insistir – veja-se DA PROVA PENAL TOMO II –, há o risco de violação do princípio da vinculação ao fim ou da alienação do fim. Fica des-legitimado o uso de determinados fluxos de dados pessoais para fins distintos aos que levaram ao seu tratamento. Dito isto, facilmente se verificam quais são os obstáculos: 1.º Não envio de dados pessoais de investigação (fluxos informacionais e comunicacionais, informático-digitais) por inexistirem garantias adequadas da sua protecção; 2.ºNão envio por ausência de garantia de cumprimento do princípio da vinculação ao fim; 3.ºNão envio dos dados porque o crime sob investigação é "irrelevante" e não justifica, em níveis de adequação, necessidade, proporcionalidade (princípio da proporcionalidade lato sensu ou da proibição de excesso) o seu envio.

12 – Vários autores partilham da opinião de que quando se trata de Cibersegurança esta apenas é possível se o sistema não estiver ligado à rede, ou seja, não existirá defesa possível, se este estiver ligado à rede. Concorda com este entendimento? Justifique.

Trata-se, como todo o respeito por tais autores, de uma opinião que não podemos subscrever. Não se ignore todo o fenómeno da "cibercriminalidade" ou "criminalidade informático-digital", já que o problema coloca-se tanto nas "intranet" como nas "extranets". A cibersegurança deve ser possível – em níveis medianamente aceitáveis – quer quando estamos "off" ou "on" a uma rede publicamente acessível de comunicação à distância ou de fornecimento de serviços electrónicos. De facto, exige-se um nível mínimo de segurança no "ciberespaço", mas isso não corresponde a dizer-se que ele existe em absoluto ou inexiste. Tem de existir um nível mínimo, embora de saiba que alguns cibercriminosos conseguem "vitrificar" toda a nossa vida. São excepções que não fazem regra. Os fornecedores de serviços de internet e das TIC têm vindo a implementar medidas adequadas. O mesmo se diga ao nível dos vários "softwares" que colocamos nos variados instrumentos electrónico-digitais. Em todos eles há mecanismos de segurança. Todavia, a primeira e última palavra permanece no operador. Se verifico que um site não é fidedigno e me aventuro para o mesmo, estou a correr um risco querido, sabendo que isso pode ser fatal. Em geral, todos os "actores" deste mundo do "dos fluxos electromagnéticos" têm contribuído com medidas para atenuar os ataques. Aliás, a capacidade de remoçamento da internet é uma das suas características. A internet vai refazendo e reelaborando as suas exigências de segurança. Disso não tenhamos dúvidas. A cada anti-vrus um novo vírus, a cada vírus um novo anti-vírus. Tudo isto num jogo de sombras ou de espelhos.

13 – A constante demanda da prevenção obriga-nos a questioná-lo acerca da possibilidade da mesma. Considera ser possível a prevenção quando falamos de ameaças informáticas, em constante evolução e transmutação? Como perspetiva a prevenção deste fenómeno criminal?

Devo sublinhar, porque isso é ignorado ou esquecido por alguns, que não é possível, em Portugal, acções proactivas ou preventivas com controlo dos fluxos informacionais e comunicacionais dos cidadãos sem que haja consentimento dos mesmos e fora de um processo criminal "em curso". Não se ignore a Constituição da República de 1976 e não se leia a mesma de forma inviesada. Há mesmo, é bom sublinhá-lo, no nosso país, algumas acções de prevenção, musculadas e proactivas, de duvidosa constitucionalidade que, de tempos a tempos, sob a sombra de governos "menos escrupulosos" (porque o

Estado tem se ter orgulho de ter um padrão ético-social mais elevado, visto representar todos os cidadãos e não desconfiar deles e, se o fizer, fá-lo, atribuindo-lhe a garantia processual penal da presunção de inocência…). Em matéria informática, como já o escrevi (nas duas obras citadas), as acções encobertas no ciberespaço são inconstitucionais. Sem mais. Leia-se, mais uma vez, o artigo 34.º, n.os 1 e 4, da CRP 1976. Também algum registo de voz e imagem o é, em acções de prevenção, como também já o escrevemos. Portanto, não se nega que a mutabilidade tecnológica pode ser um forte obstáculo ao combate das ciberameaças. Todavia, isso não é obstáculo, já que também as técnicas de investigação da cibercriminalidade – felizmente – vão mudando. O que se exige é gente jovem (ou não), com abertura de espírito, apta a uma contínua aprendizagem, com alguma curiosidade informática, e magistrados e polícias dinâmicos e abertos às múltiplas e novas formas de investigação criminal nesta área específica. A prevenção deste fenómeno criminal vai ocorrer perante um "voltar atrás", ou seja, usando de uma imagem, "devolver os 'magalhães'", fornecer formação cívica, informática e social, e, depois, se o erário público ainda o suportar, voltarem novamente os fornecimentos. Não se podem queimar etapas. Tem de educar-se para a cidadania tecnológica e sensibilizar os utilizadores de que a internet é tremendamente injusta e glutona já que come tudo e vomita tudo, a cada necessidade de informação ou de repasto. Primo, consciência informático-digital. Secundo, formação e utilização informático-digital.

14 – Quais os desafios futuros que a Cibercriminalidade apresentará aos Estados em geral?

Os principais desafios que a cibercriminalidade coloca aos actuais Estados prendem-se com a manutenção da integridade de sistemas informáticos que são imprescindíveis à vida em sociedade, mormente ao nível das redes energéticas, das redes hospitalares, das redes bancárias, de transporte, água, etc. Conclui-se que um Estado pode ficar completamente destruído ou paralisado com um ciberataque. Imagine-se o tráfego aéreo em que um vírus ilude a verdadeira posição dos aviões. Imagine-se um sistema informático manipulado que aumenta perigosamente as medidas de cloro na água. Imagine-se o tráfego de comboio baralhado e em sentido contrário. Imagine-se os semáforos a serem informaticamente viciados. Depois, o Estado "Olho Gordo" ou "big brother" está aí. Veja-se, por exemplo, o "chip na matrícula". Alguém terá dúvida da violação do princípio da vinculação ao fim ao serem usados tais dados – apesar de a lei o proibir – para descortinar se um dado criminoso esteve perto do local do crime!? O principal desafio dos Estados é conseguirem, dada a ausência de regulação da internet,

um são equilíbrio nessa plataforma informações e comunicacional universal, imparável e em constante rejuvenescimento.

14.1 – No caso do Estado Português, ainda pioneiro nestes caminhos, qual o caminho a seguir para garantir a Cibersersegurança aos seus cidadãos?

O Estado Português tem de começar por estar mais atento. Sobretudo, ao mundo académico. De facto, basta dar um exemplo. É usual, nos nossos meios de comunicação, dizer-se que o "cyberstalking" não é criminalmente punido entre nós e nunca ninguém estudo o assunto. Ora, nem uma nem outra coisa são verdadeiras. No nosso caso, já em 2009 apresentamos uma proposta de criminalização e encontramos no direito positivo a possibilidade de criminalizar, sem violação do princípio da legalidade e tipicidade, tais tipos de condutas. Estuda-se pouco em Portugal e comenta-se muito, fica-se por um nível terrivelmente superficial e lacunar. O Estado Português tem de levar a cabo acções de educação para a cidadania electrónica. Depois, tem de, uma vez por todas, deixar de "chantagear" e "lamuriar-se" da ineficácia dos órgãos de polícia criminal e, de um modo cabal, fornecer-lhes os meios técnicos e não lhe cercear a vontade. Tenho notado – e talvez o ISCPSI tenha nisso uma quota-parte de contributo elevado – um aumento da competência dos nossos oficiais e agentes dos órgãos de polícia criminal (in casu, naturalmente, da PSP). De uma vez por todas, cria-se uma super-entidade agregadora, como se disse supra, e estou certo que os proveitos e proventos serão enormes para o país e vida dos cidadãos. O que não é válido no mundo real não é o no mundo virtual. Esta é a mensagem essencial.

15 – Caso represente um serviço ou força dessegurança ou qualquer serviço com competências de segurança nestes domínios, qual o principal contributo que esse serviço em particular pode dar em matéria de Cibersegurança?

Neste caso, não poderei – de todo – responder, já que não me enquadro no perfil pressuposto pela questão.

<u>Notas/sugestões/opiniões:</u>

*Envio-lhe esta versão. Pedia-lhe para dar uma vista de olhos. Caso entenda que deva desenvolver ou não ficou respondida, cabalmente, qualquer pergunta, não hesite em me pedir nova versão.**Salvo melhor opinião, estas são as respostas que considero mais adequadas e em perfeita honestidade intelectual e na estreita medida dos meus conhecimentos.***

APÊNDICE 6

Entrevista a Pedro Verdelho

APÊNDICE 6

Entrevista Exploratória n.º 6

A presente entrevista enquadra-se no âmbito da realização de uma Dissertação de Mestrado que aborda a Cibersegurança no quadro da Cooperação Policial Internacional. Sob a orientação da Exma. Sr.ª Professora Doutora Ana Paula Brandão, surge esta investigação no seguimento do Mestrado Integrado de Ciências Policiais e Segurança Interna ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna proposta pelo abaixo identificado como Entrevistador.

Com este método de recolha de informação queremos salientar o vínculo qualitativo da nossa investigação. Apraz-nos, desta feita, agradecer a Vossa Excelência o contributo que queremos desde já classificar como imprescindível.

Assim, pedimos-vos que tratem as vossas respostas com a maior sinceridade e objectividade. Não olvidamos o caráter anónimo/confidencial que a sua entrevista poderá assumir por razões axiomáticas. Ao tema está inerente uma natureza interdisciplinar desde as Ciências Policiais passando pela Ciência Política e Relações Internacionais e pelo Direito Penal, até áreas do saber mais técnico e específico relacionado com as Tecnologias de Informação e Comunicação; pedimos-lhe que dê o seu sábio contributo mesmo que não se reveja com a área de saber correspondente à questão.

*Sinta-se à vontade para em qualquer altura da realização desta entrevista acrescentar sugestões, pontos de vista e opiniões de assuntos que relativos ao tema que não venham plasmados nesta entrevista.

Guião da Entrevista

Nome: *Pedro Verdelho.*

Cargo: *Procurador da República – Coordenador do Gabinete Cibercrime de Procuradoria-Geral da República.*

Entidade: *Procuradoria-Geral da República.*

Data/Hora: *18/04/2012*

Local: *Respondida via e-mail.*

Duração:

Entrevistador: *Nélson Silva (Aspirante a Oficial de Polícia), XXIV Curso de Formação de Oficiais de Polícia da Polícia de Segurança Pública, nº 2405/153561. Comando: Instituto Superior de Ciências Policiais e Segurança Interna.*

1 – No que concerne à atuação Estadual, considera o fenómeno da Cibercriminalidade como prioritário? Em que aspetos e a que nível?

A cibercriminalidade tem sido declarada como uma das formas de criminalidade que importa combater. O programa do Governo anterior assim o dizia expressamente, tendo até sido prometida a criação de unidades policiais, na PSP e GNR, especializadas na matéria. Assim não aconteceu. Por outro lado, a opção pública, de declaração de

importância, foi também revelada pela adopção de lei especial nesta matéria e pela adesão a instrumentos internacionais, que forma transpostos para a lei interna.

1.1 – Do mesmo modo, agora, relativamente à atuação Internacional considera o mesmo fenómeno prioritário? Em que aspetos e a que nível?

Várias organizações internacionais têm declarado o cibercrime uma prioridade. Assim acontece com a ONU, que inseriu a temática na sua agenda em matéria de política criminal; também com a OCDE e o grupo dos países do G8, que fizeram declarações políticas a este propósito. A União Europeia adoptou documentos vinculativos para os Estados Membros nesta matéria e o Conselho da Europa elaborou e abriu à assinatura a Convenção de Budapeste, o mais importante tratado internacional a este propósito.

2 – Consideramos que a Cooperação Internacional é urgente e necessária na prevenção e combate das Ciberameaças. Partilha desta nossa opinião? Porquê?

A criminalidade nas redes de comunicação é, pela sua própria natureza, internacional. Por definição, as comunicações atravessam mais que um país, usando em simultâneo serviços da sociedade de informação de diferentes pontos do globo. Na Internet não há fronteiras nem barreiras. O mesmo acontece com as actividades criminais desenvolvidas nas redes: ocorrem em simultâneo em várias jurisdições, supondo que as autoridades judiciais e policiais de cada uma delas se socorram umas das outras, para investigar, promover o processo e julgar com eficácia. Por tudo, a cooperação internacional é uma das variáveis essenciais em qualquer actividade de investigação criminal em matéria de cibercriminalidade.

3 – Quais os instrumentos e estruturas de cooperação a nível Internacional de prevenção e combate à Cibercriminalidade que considera vitais e realmente funcionais?

A cooperação internacional na investigação de cibercriminalidade não se compadece com a tradicional morosidade dos instrumentos clássicos de cooperação judicial internacional, dependente da emissão de cartas rogatórias que cumprem percursos formais e prolongados no tempo. Por isso, assumem especial importância os modernos mecanismos de cooperação criados pela convenção de Budapeste, que criou novas vias e novas modalidades de cooperação expedita. Neste contexto, sublinha-se a criação de uma rede de contactos destinada a facilitar a cooperação, disponível 24 horas por dia, 7 horas por semana.

Esta rede, que Portugal já integra (o ponto de contacto está baseado na Polícia Judiciária), permite por exemplo, por via de contactos informais, solicitar a congéneres de

todo o mundo a preservação urgente de dados de tráfego que, de outra forma se perderiam. A serem utilizadas as vias convencionais não seria possível pedir a preservação em tempo destes dados.

O ponto de contacto está baseado na Polícia Judiciária mas deverá providenciar cooperação a países terceiros mesmo que haja necessidade de intervenção judiciária. Por outro lado, no sentido oposto, deverá apoiar outros órgãos de polícia criminal nacionais, se estes tiverem que recorrer a algumas das medidas expeditas de cooperação internacional.

.

4 – As estruturas de cooperação estão coordenadas de forma eficaz? Promove-se uma real cooperação de combate à Cibercriminalidade ou qualquer outro fenómeno criminal transnacional?

Ver questão anterior.

5 – Considera que existe efetivamente uma Cooperação Policial Internacional no combate à Cibercriminalidade? Quais as entidades envolvidas que considera relevantes? Quais os obstáculos e progressos?

Ver questões anteriores.

6 – Acredita que existe um défice de cooperação e coordenação entre as estruturas internacionais? De que modo?

A natureza intrínseca da cooperação criminal (que tem sempre na base acordos voluntários entre Estados) não potencia a coordenação entre os diversos actores – *maxime* os Estados -, fora dos quadros institucionais. Neste contexto, institucional, há com frequência grande harmonização das posições. Por exemplo no seio da UE, tem havido grande esforço de coordenação das opções dos Estados em matérias de cibercriminalidade.

Fora das instituições internacionais, a coordenação pode ser mais dificultada pelas diferentes sensibilidades dos vários Estados do mundo. Não é fácil, por exemplo, conciliar qualificações jurídicas entre todos os Estados: há países onde certos factos constituem crime e, exactamente os mesmos factos, para outros Estados são lícitos.

Esta diferente perspectiva cria dificuldades à cooperação: se um facto é crime num Estado e não é no outro, se este último for solicitar a cooperar com o primeiro, não o poderá fazer, porque os factos em causa não são por ele considerados crime. Esta situação é muitíssimo frequente na actualidade.

7 – Existindo o anterior défice, considera que esta situação fará perigar um eficaz combate e prevenção da Cibercriminalidade? Justifique.

Ver questão anterior.

8 - A União Europeia, enquanto ator de segurança, tem como missão providenciar e tornar efetiva a cooperação para combater o Cibercrime. De entre as várias medidas implementadas quais as que realmente promovem e efetivam a cooperação policial?

Esta questão deverá ser colocada às estruturas policiais.

9 – Considera que a EUROPOL e a INTERPOL realmente promovem a cooperação policial e partilha de informações? Quais as dificuldades e resultados positivos já alcançados nestas matérias?

Esta questão deverá ser colocada às estruturas policiais.

9.1 – Estas estruturas trazem um valor acrescentado ao combate da Cibercriminalidade? De que modo?

Esta questão deverá ser colocada às estruturas policiais.

9.2 – A um nível de aplicação prática, considera que essas estruturas têm impacto a nível da atuação nacional no combate às Ciberameaças? Fundamente.

Esta questão deverá ser colocada às estruturas policiais.

10 – Considera que se verifica o princípio da cooperação mútua em Portugal no geral? Existe cooperação entre as demais entidades com competências para prevenir e combater o Cibercrime atualmente no nosso País? Em que medida?

Esta questão deverá ser colocada a quem tenha responsabilidade nas estruturas operacionais.

11 – Transpondo a questão agora para o nível internacional, considera existir uma permuta de informações entre os níveis nacional e internacional? Quais os obstáculos e avanços?

Esta questão deverá ser colocada a quem tenha responsabilidade nas estruturas operacionais.

12 – Vários autores partilham da opinião de que quando se trata de Cibersegurança esta apenas é possível se o sistema não estiver ligado à rede, ou seja, não existirá

defesa possível, se este estiver ligado à rede. Concorda com este entendimento? Justifique.

Esta questão deverá ser colocada às estruturas de segurança.

13 – A constante demanda da prevenção obriga-nos a questioná-lo acerca da possibilidade da mesma. Considera ser possível a prevenção quando falamos de ameaças informáticas, em constante evolução e transmutação? Como perspetiva a prevenção deste fenómeno criminal?

Concordo, em absoluto, com a necessidade de prevenção como a forma mais eficaz de encarar as "ciberameaças". Esta prevenção passa sobretudo pela educação dos utilizadores das redes. Mas passa também pelo incremento de medidas de segurança.

14 – Quais os desafios futuros que a Cibercriminalidade apresentará aos Estados em geral?

O grande desafio será o da dimensão: no futuro próximo, uma boa parte da tradicional criminalidade transferir-se-á para o ambiente digital, que providencia aos criminosos velocidade de acção, anonimato e segurança.

14.1 – No caso do Estado Português, ainda pioneiro nestes caminhos, qual o caminho a seguir para garantir a Cibersersegurança aos seus cidadãos?

Ver questão 14.

15 – Caso represente um serviço ou força dessegurança ou qualquer serviço com competências de segurança nestes domínios, qual o principal contributo que esse serviço em particular pode dar em matéria de Cibersegurança?

Não é aplicável..

Notas/sugestões/opiniões:

Muito obrigado pelo preenchimento da presente entrevista. Caso esta entrevista revista, por qualquer motivo, caratér anónimo, garantimos-lhe que será dado o devido tratamento em função desse facto.

Agradecemos mais uma vez, e muito sinceramente, a atenção e tempo disponibilizados na realização desta entrevista.

APÊNDICE 7

Entrevista a Adam Palmer

APÊNDICE 7

Exploratory Interview n.º7

This interview fits into a Master's Thesis about Cybersecurity within the framework of International Police Cooperation. Under the orientation of PhD. Ana Paula Brandão, this research comes within the Integrated Master's Degree of Police Sciences and Internal Security administered by Higher Institute of Police Sciences and Internal Security (ISCPSI), a University of Portuguese's Public Security Police by the Interviewer identified below. This interview is a data collection technique for the master research project about international police cooperation and cybercrime, of the Master Programme in Police Studies .

We are pleased to thank your magnificent contribution that we classify as essential. So we ask you to treat your answers with the most sincerity and objectivity. There is absolutely no problem to classify your interview as "classified" if you wish so.

At this issue is an inherently interdisciplinary nature ranging from the Policial Science, passing by Political Science and International Affairs crossing Criminal Law and ending in areas of more technical and specifically related to Information and Communications Technologies, nevertheless, we expect your wise input to all questions even if that area isn't your knowing curriculum.

*Feel free, in any moment, to talk about something that you consider important for this issue that isn't in questions

Interview Guide

Name: *Adam Palmer*

Position*: Norton Lead Cybersecurity Advisor*

Organization: *Symantec*

Date: *15/03/2012*

Location: *Respondida via e-mail.*

Duration: ---

Interviewer: *Nélson Silva, XXIV Course of ISCPSI of Portuguese's Public Security Police, nº 2405/153561. Higher Institute of Police Sciences and Internal Security*

1. How do you define the cyber threats?

Cybercrime fits into two main categories: 1.) Old crimes committed in new faster ways using technology and 2.) Misuse of technology systems. In addition to cybercrime there are also cyberthreat issues related to actions by national governments. This raises the issue of defining the boundary between cybercrime (a police issue) and cyberwar (a military issue).

2. In your opinion, what are the main features of cybercrime at the present times?

Cybercrime is an organized criminal threat to the global economy and justice system. The Internet is now a major component of the global economy and a threat to its security, and the security of its users, is a direct threat against the global economy. The scale, complexity, and speed of cybercrime is also a significant challenge for law enforcement that requires increased cooperation and technological capability. Today, it is clear that cybercriminals have become increasingly sophisticated and targeted. While they previously used to distribute a few threats to a large number of people, they are now micro distributing millions of distinct threats to smaller, unique groups of people. Most of today's threats are polymorphic – which means each variant is ever so slightly different from the other in order to evade detection.

3. Do you consider that the fight against cybercrime is a priority for states, both at national and international levels?

Cybercriminals move at the speed of light but law enforcement move at the speed of law. Cybercrime is increasingly gaining attention in the world, but more can be done. Some governments also have other important concerns so cybersecurity may not have adequate funding or resources. Laws must be updated to address new forms of crime in cyberspace. Most governments acknowledge that cybersecurity is an important function in protecting their citizens.

4. What are the main obstacles in the fight against cybercrime?

Global cooperation and technical capability remain a challenge for law enforcement to adequately fight cybercrime. This is a crime that quickly crosses international borders. And requires global cooperation. Police must also have an advanced understanding of the technology involved in cases and how to properly collect digital evidence. One of the biggest challenges faced by law enforcement in preventing cybercrime is the enormous scope of the problem. With so many victims in many different countries, police can successfully stop one cybercriminal but still be left with thousands more cases. Cybercrime is a growing threat that requires significantly more resources than are currently being allocated to curb it.

5. Do you agree with the statement that international cooperation is relevant for the prevention of cybercrime due its transnational dimension?

Yes, I agree with this statement. As noted above, this is a borderless crime requiring global cooperation from police having jurisdiction in the areas that the crime touches. It is not uncommon in cybercrime cases for the victim and criminal to be on different continents and for the

criminal to use technology located on a third continent. To collect this evidence and effectively investigate the case, the police must cooperate with their global counterparts.

6. In your opinion, what are the most efficient international institutions and mechanisms in the fight against cybercrime?

The private sector and non-profit groups play a large role in assisting law enforcement in the fight against cybercrime. I am co-located at the National Cyber Forensic Training Alliance (NCFTA) in the USA. This is a non-profit that serves as a cooperation center between industry and law enforcement and has been very effective. This idea of public-private partnership is actually at the core of the Norton Cybersecurity Institute, a program started by Norton 2 years ago to help support law enforcement in the fight against cybercrime. By supporting police training and cooperation globally, the Norton Cybersecurity Institute helps police build the skills necessary to fight cybercrime.

7. How do you assess the role of Europol and Interpol in the prevention and fight against cybercrime?

Global cooperation is important and both of these groups represent a great forum for increasing cooperation. Because international laws in cyberspace can vary widely, cooperation can sometimes be a challenge. However, both of these groups provide an excellent forum for training and capacity building. Global cooperation continues to be the main focus of need and concern among law enforcement. Cybercriminal attacks move freely across international borders. Success against these attacks can only be achieved through international cooperation. It is extremely frustrating to track a criminal to a country, only to have that suspect hide behind an international border that is outside the jurisdiction of the foreign police tracking the suspect.

8. Do you consider that was useful create a new international police to face this issues and name it like Cyberpol for example?

Groups like EUROPOL and INTERPOL already provide a powerful forum for global cooperation against cybercrime while respecting individual national government differences. Cybercrime is a global epidemic that can't be solved by one company or law enforcement agency alone; keeping the Internet safe is a shared responsibility and needs to be done effectively with public-private partnership. That's why we launched a public private partnership program called the Norton Cybersecurity Institute, a collaboration between law enforcement, consumer safety groups and Norton. The Norton Cybersecurity Institute is a global initiative to support and win the fight against cybercrime by providing law enforcement with training, technical expertise, and improved global cooperation.

Through training and global collaboration, the Norton Cybersecurity Institute will help law enforcement in their efforts to catch and prosecute cybercriminals successfully.

9. Do you consider that the coordination between the international and national levels is effective? Why?

Some governments make little effort to stop criminal gangs operating within their borders. However, this is not a unique problem that applies only to cybercrime. These same issues are generally persistent to some degree across all criminal activities. These countries are not necessarily supporting cybercrime any more than they are supporting other forms of crime. There is a law enforcement capability problem that must be resolved across all segments of crime. We must work to increase police capacity and cooperation at the national and international level, but also understand that these problems are not necessarily unique to cybercrime.

10. In your opinion, what are the main challenges and future trends of cyberthreats?

New complex attacks are the most recent and visible examples of what Symantec has been observing for some time now: attackers motivated by the profits to be gained from cybercrime - from intellectual property theft to stealing consumer bank accounts- criminals are taking advantage of the increasingly digital world. Cyber security issues are hitting headlines. There are three implications to the increase in such attacks: these threats aren't going away, they are becoming more sophisticated, and security is everyone's responsibility. With the explosion of devices, systems, users, and access, every user must be educated and aware of his responsibilities. Today, critical information assets are dispersed across the cloud, smart devices and social media, bringing new challenges in security. To prevent targeted attacks, organizations need a security strategy that is risk-based and policy-driven, information-centric and operationalized across a well-managed infrastructure. Users need to be educated of these threats and keep updated security.

Mobile security threats continue to rise with 10% of mobile users reporting in a recent survey that they had become victims of mobile cybercrime last year. This will continue to increase and likely spread to other Internet connected devices. Cyberspace is now ruled by tablets, smart phones, Internet connected TV's and thousands of other smart connected devices that help consumers access personal information regardless of where they are. Mobile crime is becoming a significant threat, and Norton observed a 42 per cent increase in mobile vulnerabilities in 2010. From malicious, but real-looking apps for

Android phones that are put up on app stores for users to download, to malicious gaming applications that can track users' movement, making it possible to steal from their physical property when they are not present, cybercriminals are clearly following the crowds to newer platforms to make a profit.

11. Many authors consider that Cibersecurity in only possible if the system isn´t connected to the network, in other words, there will be no possible defense if the system is connected. Did you agree with this position? Justify.

Technology brings many great benefits to our lives but it needs to be used safely. No system is 100% secure but by following good security practices the risk of being victimized can be greatly reduced. Avoiding technology is the wrong answer. Computers don't commit crimes, people do. We need to focus on stopping criminals, not missing the benefits of technology. New devices and complex attacks by cybercriminals can stretch the technical capabilities of investigators. Technology does change, but ignoring its impact on citizens is not an effective solution. Some technology, such as social networking, may change popular platforms over time, but the idea of social networking remains a part of modern culture. However building barriers against new technology only denies the public the benefits of technology because a few abuse it.

12. What about the prevention of this type of e-criminality? Is it possible to prevent a phenomenon in constant evolution and mutation? How you prospect the criminal prevention of this phenomenon?

One of the biggest challenges faced by law enforcement is the enormous scope of the problem. Every day of the past year, over 1 million online adults in 24 countries experienced cybercrime. This can also be broken down to 50,000 victims per hour, 820 victims per minute, or 14 victims every second. With so many victims in many different countries, police can successfully stop one cybercriminal but still be left with thousands of more cases. The police do a great job trying to stop cybercrime but the problem requires significantly more resources than are currently being devoted to stop it.

Only 21% of victims in a recent Norton study reported the cybercrime to law enforcement. This also creates a significant problem for police and prosecutors. Some prosecutors will only accept cases that exceed a certain amount of victims or high level of damages. However, what we've observed is that most cybercrime involves a relatively small amount individually spread across many victims. However, failure to report cybercrime prevents law enforcement from effectively addressing the problem.

In conclusion, we must devote more resources to training an education of police to fight cybercrime while also continuing to educate the public about good security practices and reporting cyber crime issues.

13. Portugal is beginning to take its first steps in a really Cybersecurity Politic. Our rising in this issue starts with the ratifying of International Cybercrime Convention. In order to finish we want to know what would be more wisely for Portugal in this young journey facing Cibersecurity for real. Give us your advise!

Cybercrime is a global epidemic that can't be solved by one country or law enforcement agency alone; keeping the Internet safe is a shared responsibility. Focus on cooperation and outreach to trusted partners. Improve laws to not focus on a specific technology that may change, but rather to address the new forms of digital evidence and police challenges in cyberspace.

14. Is there anything else you would like to say about the topic that was not covered in these questions?

We often focus solely on government or business issue in cybercrime, however, the individual user should not be forgotten. The individual Internet user needs to follow good security practices not only for their own protection but also because of the critically important contribution that each individual makes to the security of the entire Internet eco-system. A lack of security at the individual level risks an entire government or corporate network. An individual infected device can also be used as part of a botnet to harm other individual users. For these reasons, the individual Internet user remains important to maintaining a safe Internet for everyone.

Opinions / suggestions / advices:

APÊNDICE 8

Entrevista a Andrea Dufkova

Apêndice n.º8

Exploratory Interview n.º8

This interview fits into a Master's Thesis about Cybersecurity within the framework of International Police Cooperation. Under the orientation of PhD. Ana Paula Brandão, this research comes within the Integrated Master's Degree of Police Sciences and Internal Security administered by Higher Institute of Police Sciences and Internal Security (ISCPSI), a University of Portuguese's Public Security Police by the Interviewer identified below. This interview is a data collection technique for the master research project about international police cooperation and cybercrime, of the Master Programme in Police Studies .

We are pleased to thank your magnificent contribution that we classify as essential. So we ask you to treat your answers with the most sincerity and objectivity. There is absolutely no problem to classify your interview as "classified" if you wish so.

At this issue is an inherently interdisciplinary nature ranging from the Policial Science, passing by Political Science and International Affairs crossing Criminal Law and ending in areas of more technical and specifically related to Information and Communications Technologies, nevertheless, we expect your wise input to all questions even if that area isn't your knowing curriculum.

Interview Guide

Name: *Andrea Dufkova*

Position: *Technical Competence Department*

Organization: *ENISA*

Date/Time: *15/03/2012*

Location: *Respondida via e-mail.*

Duration: ---

Interviewer: *Nélson Silva, XXIV Course of ISCPSI of Portuguese's Public Security Police, nº 2405/153561. Higher Institute of Police Sciences and Internal Security*

1. **How do you define the cyber threats?**

It is not easy to give a general definition of what is considered to be a cyber threat. Many different definitions are used, depending on for instance the scope of the organisation. A consumer for instance has a completely different view on cyber threats and security than military of law enforcement organisations. One possible way to define a cyber threat is to describe it as a threat or risk against a computer system or a network or using a computer system or network as a tool to execute the threat. From the legal point of view, a definition of cyber threats could be derived from the definitions given in the Council of Europe Convention on Cyber Crime – Explanatory Report, see in particular par. 35 (http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm). For a definition of some

specific attacks against information systems, reference can be made to the Council Framework Decision on attacks against information systems 2005/222/JHA (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF) which is currently under revision (see Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=EN&type_doc=COMfinal&an_doc=2010&nu_doc=517) or also to the Council of Europe Convention on Cyber crime (http://conventions.coe.int/treaty/en/treaties/html/185.htm).

2. **In your opinion, what are the main features of cybercrime at the present times?**

Cybercrime is basically a cyber threat which has crime as it's main objective.

3. **Do you consider that the fight against cybercrime is a priority for states, both at national and international levels?**

We see that in the last years cybercrime becomes more and more a 'hot topic', both on national level and international level. On a European level various initiatives are taken, such as the Digital Agenda and the EU Internal Security Strategy, putting the fight against cybercrime on the agenda, also, there is Proposal for a Directive on attacks against information systems (http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=EN&type_doc=COMfinal&an_doc=2010&nu_doc=517). In addition, an increasing number of countries are developing and implementing cyber security strategies and other measures to prevent and fight cybercrime.

4. **What are the main obstacles in the fight against cybercrime?**

There are a lot of actors active in the fight against cybercrime. Now it is key to make all these efforts join together, find synergies and overcome barriers. One example is the collaboration between Law Enforcement Agencies and CERTs. Both communities are working and putting efforts in this fight, but they could assist each other more (in certain countries) than they do now. There are operational and legal barriers to this. - Legal challenges, such as definitions of different types of computer and network misuse, balancing privacy and response to cyber crime, issue of jurisdiction, legal framework for police and judicial cooperation, etc. (see also: ENISA study 'A flair for sharing - encouraging information exchange between CERTs'. Link: Http://www.enisa.europa.eu/activities/cert/support/legal-information-sharing);

- Lack of training/resources in dealing with cyber crime and computer evidence; - Issues related to computer evidence (e.g. volatility, huge amount of information, etc.); - Fast development and usage of newer and more sophisticated technologies; - High number of unreported cyber crime cases.

5. **Do you agree with the statement that international cooperation is relevant for the prevention of cybercrime due its transnational dimension?**

International cooperation is vital for the prevention of and fight against cybercrime, since cybercrime by nature cannot be confined to national boundaries. Cross-border cooperation and collaboration between different stakeholders should be stimulated and supported as it is a crucial factor for the success of the fight against cybercrime.

6. **In your opinion, what are the most efficient international institutions and mechanisms in the fight against cybercrime?**

There are different organisations active in this field. Each of them has their role to play and it is the combination of all of these efforts that gives strength to a combined fight against cybercrime. The 24/7 mechanism, also foreseen by the Council of Europe Convention on cyber crime, is a particular important mechanism for the fight against cybercrime.
Another mechanism that has proved to be very effective is the cooperation in the CERT community. They have good cross-border communication and collaboration.

7. **How do you assess the role of Europol and Interpol in the prevention and fight against cybercrime?**

ENISA is not in the position to answer this question.

8. **Do you consider that was useful create a new international police to face this issues and name it like Cyberpol for example?**

ENISA is not in the position to answer this question.

9. **Do you consider that the coordination between the international and national levels is effective? Why?**

The coordination between the international and national levels is particularly important for the prevention and fight against cybercrime. It is difficult to assess its effectiveness without referring to a specific country. What is definitively welcome are the efforts both at national, supranational and international level to reach the highest level of effectiveness.

10. In your opinion, what are the main challenges and future trends of cyberthreats?

Among the others, the following challenges can be identified: - new technologies and business models continuously being introduced - the use of old technologies is being extended in ways that were never envisaged when they were first developed - new business models seriously push existing concepts and regulation to their limits (see, e.g. cloud computing) - deliberate attempts to cause harm Reference: 'Cyber security: future challenges and opportunities', http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities Next to that I would also like to refer to 'Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices', http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime, a report that makes some conclusions and recommendations on the topic of the fight against cybercrime.

11. Many authors consider that Cibersecurity in only possible if the system isn´t connected to the network, in other words, there will be no possible defense if the system is connected. Did you agree with this position? Justify.

The 'Digital Agenda for Europe' aims to achieve a new digital single market by the year 2020. One of the main goals of this agenda is to provide Internet access to all Europeans. Along with this planned increased connectivity of European citizens, they have also become increasingly dependent on IT.
Our society relies heavily on systems connected to the network. Solutions are in place and will be further developed in order to protect systems connected to the network. Proactive detection of network security incidents is an example (for more information please see ENISA Report on Proactive Detection of Network Security Incidents, http://www.enisa.europa.eu/activities/cert/support/proactive-detection/)

12. What about the prevention of this type of e-criminality? Is it possible prevent a phenomenon in constant evolution and mutation? How you prospect the criminal prevention of this phenomenon?

Both prevention of and the fight against cyber crime are important. From the legal point of view, to prevent and fight at the best a phenomenon on constant evolution and mutation it is important to develop legislation inspired to the principle of technology-neutral language, "so that the substantive criminal law offences may be applied to both current and future technologies involved" (See Council of Europe Convention on Cyber Crime – Explanatory

Report, see in particular par. 36 (http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm).

13. **Portugal is beginning to take its first steps in a really Cybersecurity Politic. Our rising in this issue starts with the ratifying of International Cybercrime Convention. In order to finish we want to know what would be more wisely for Portugal in this young journey facing Cibersecurity for real. Give us your advise!**

Close dialogue with the Council of Europe and exchange with other countries of good practices on the implementation of the Convention can be key elements for the success. ENISA can be a broker in this exchange and has a lot of material that can help.

Is there anything else you would like to say about the topic that was not covered in these questions?

You might find interesting information for the thesis in the material available on the ENISA website: http://www.enisa.europa.eu/ For material in the field of CERTs, please see in particular: http://www.enisa.europa.eu/activities/cert

Opinions / suggestions / advices:

In 2012 ENISA is working on two good practice guides on the fighting against cybercrime (operational and legal/regulatory aspects). The results of these studies are expected to be published on the ENISA website towards the end of the year.

I thank you for your valuable and useful contribution for my research.

APÊNDICE 9

Entrevista a Eneken Tikk

APÊNDICE 9

Exploratory Interview n.º9

This interview fits into a Master's Thesis about Cybersecurity within the framework of International Police Cooperation. Under the orientation of PhD. Ana Paula Brandão, this research comes within the Integrated Master's Degree of Police Sciences and Internal Security administered by Higher Institute of Police Sciences and Internal Security (ISCPSI), a University of Portuguese's Public Security Police by the Interviewer identified below. This interview is a data collection technique for the master research project about international police cooperation and cybercrime, of the Master Programme in Police Studies .

We are pleased to thank your magnificent contribution that we classify as essential. So we ask you to treat your answers with the most sincerity and objectivity. There is absolutely no problem to classify your interview as "classified" if you wish so.

At this issue is an inherently interdisciplinary nature ranging from the Policial Science, passing by Political Science and International Affairs crossing Criminal Law and ending in areas of more technical and specifically related to Information and Communications Technologies, nevertheless, we expect your wise input to all questions even if that area isn't your knowing curriculum.

*Feel free, in any moment, to talk about something that you consider important for this issue that isn't in questions

Interview Guide

Name: *Eneken Tikk-Ringas*

Position: *Independent Researcher*

Organization: *(CCDCOE)*

Date/Time: *01/04/2012*

Location: *Tallinn, Estonia*

Duration: *Respondida via e-mail*

Interviewer: *Nélson Silva, XXIV Course of ISCPSI of Portuguese's Public Security Police, nº 2405/153561. Higher Institute of Police Sciences and Internal Security*

1. **How do you define the cyber threats?**

I understand cyber threats as potential unwanted/unexpected impact on data, information and services run on or via information infrastructure, on the underlying infrastructure itself as well on activities or objects relying on the former.

2. **In your opinion, what are the main features of cybercrime at the present times?**

With all the historical factors still present (personal, financial motivation, youth engagement etc.), the more current and dangerous features include organized crime blending in, political motivation

behind crimes as well as subscription by States to cyber criminal services (or toleration thereof) as well as sophistication of schemes (careful jurisdiction shopping, diffused consequences, investments into avoiding attribution etc.).

3. **Do you consider that the fight against cybercrime is a priority for states, both at national and international levels?**

Yes. This activity has not been gained under control for decades and represents the main platform for most cyber incidents with significant impact to economy, society and governments.

4. **What are the main obstacles in the fight against cybercrime?**

There are several. Definitely, lack of resources and experience in some jurisdictions; information sharing in others; careful action by criminals complicates investigations; unwillingness of victims to report, low awareness of users etc. all add to it.

5. **Do you agree with the statement that international cooperation is relevant for the prevention of cybercrime due its transnational dimension?**

Absolutely. Experience of each country is valuable from at least technical perspective (legal orders are different, though), and a working cooperation facilitates and speeds up both prevention and response. Also, cooperation programmes (e.g. Taurus between NL and US) that focus on certain areas of threats and their mitigation are of huge value, as are policy coordination efforts (e.g. development of like-minded coalitions in NATo, UN GGE etc.) as they generate wider awareness, exchange of experience and better understanding that helps in real threat mitigation situation.

6. **In your opinion, what are the most efficient international institutions and mechanisms in the fight against cybercrime?**

I think the most efficient efforts are of bilateral nature (cooperation agendas between CERTs and law enforcement authorities etc.). Other than that different institutions have different strengths (Interpol hands-on handling experience, Council of Europe the cyber crime convention, UN GGE a broad mandate and willingness to engage more countries in political level, G8 steps for selected countries).

7. **How do you assess the role of Europol and Interpol in the prevention and fight against cybercrime?**

Not enough familiar to comment.

8. **Do you consider that was useful create a new international police to face this issues and name it like Cyberpol for example?**

I don't think a new organization per se would be necessary. What would be the contribution, is the first question, not the name ;)

9. **Do you consider that the coordination between the international and national levels is effective? Why?**

Question is a bit too broad – do you mean law enforcement, policies, CERTs, ISPs or legislative?

10. **In your opinion, what are the main challenges and future trends of cyberthreats?**

The trend of cultivating low awareness and lack of resources as well as overall dependence on ICTs for malicious purposes is growing. This should challenge everyone to take it all very seriously (and more concrete).

11. **Many authors consider that cybersecurity in only possible if the system isn´t connected to the network, in other words, there will be no possible defense if the system is connected. Did you agree with this position? Justify.**

Yeah :) Well, all ships would be safe never leaving the harbor and aircraft never taking off. What's the point :)

12. **What about the prevention of this type of e-criminality? Is it possible prevent a phenomenon in constant evolution and mutation? How you prospect the criminal prevention of this phenomenon?**

There are many real and useful practices of botnet takedown, attribution, extradition and prosecution. One should study those carefully and build on them. Of course, it is possible.

13. **Portugal is beginning to take its first steps in a really Cybersecurity Politic. Our rising in this issue starts with the ratifying of International Cybercrime Convention. In order to finish we want to know what would be more wisely for Portugal in this young journey facing Cibersecurity for real. Give us your advise!**

Everything starts from a strong and competent national task force. Engage all relevant authorities, develop a solid knowledge of the area, assess your domestic risks and strengths critically, build meaningful partnerships with international organizations and other nations (and be careful as different nations have very different strategic approaches and not all may be relevant/constructive to partner) and incentivize enthusiasm and synergy. It is a complex, but extremely interesting and

rewarding expertise area to develop in a country. Get tailor-made training and consultations from top experts, but be critical on how to implement their advice in the Portugese context. Good luck!!!

Is there anything else you would like to say about the topic that was not covered in these questions?

Well, I have a lot to say about everything :) I just hope we will cross paths again to follow up these discussions!

Opinions / suggestions / advices:

Wish you a successful finalization phase and good luck with your degree!

I thank you for your valuable and useful contribution for my research.

APÊNDICE 10

Entrevista a Myriam Dunn Cavelty

APÊNDICE 10

Exploratory Interview n.º10

This interview fits into a Master's Thesis about Cybersecurity within the framework of International Police Cooperation. Under the orientation of PhD. Ana Paula Brandão, this research comes within the Integrated Master's Degree of Police Sciences and Internal Security administered by Higher Institute of Police Sciences and Internal Security (ISCPSI), a University of Portuguese's Public Security Police by the Interviewer identified below. This interview is a data collection technique for the master research project about international police cooperation and cybercrime, of the Master Programme in Police Studies .

We are pleased to thank your magnificent contribution that we classify as essential. So we ask you to treat your answers with the most sincerity and objectivity. There is absolutely no problem to classify your interview as "classified" if you wish so.

At this issue is an inherently interdisciplinary nature ranging from the Policial Science, passing by Political Science and International Affairs crossing Criminal Law and ending in areas of more technical and specifically related to Information and Communications Technologies, nevertheless, we expect your wise input to all questions even if that area isn't your knowing curriculum.

Interview Guide

Name: *Myriam Dunn Cavelty*

Position: *Head of Risk and Resilience Research Group*

Organization: *Center for Security Studies, ETH Zurich (Swiss Institute of Technology)*

Date/Time: *03/04/2012*

Location: *Zurich*

Duration: *respondida via e-mail*Clique aqui para introduzir texto.

Interviewer: *Nélson Silva, XXIV Course of ISCPSI of Portuguese's Public Security Police, nº 2405/153561. Higher Institute of Police Sciences and Internal Security*

1. **How do you define the cyber threats?**

Threats and risks in and through cyberspace.

2. **In your opinion, what are the main features of cybercrime at the present times?**

Professionalization, high incentives, low cost on the side of the attacker, many low hanging fruit

3. **Do you consider that the fight against cybercrime is a priority for states, both at national and international levels?**

Yes, it should be

4. **What are the main obstacles in the fight against cybercrime?**

Attribution problem (knowing who did something bad on the internet), different legal systems, sketchy international cooperation

5. **Do you agree with the statement that international cooperation is relevant for the prevention of cybercrime due its transnational dimension?**

Yes, very much so

6. **In your opinion, what are the most efficient international institutions and mechanisms in the fight against cybercrime?**

European Cybercrime Convention, United Nations Transnational Organised Crime Convention

7. **How do you assess the role of Europol and Interpol in the prevention and fight against cybercrime?**

Both institutions are important, though not yet perfect

Europol's primary function is to support the operational activities of national law enforcement officials and recently extended to include the fight against cyber-crime. In furtherance of this its representatives facilitate the exchange of information, provide analyses of criminal intelligence, generate strategic reports on trends and patterns of criminal activity, and provide technical expertise for ongoing investigations within the EU. It is likely Europol will eventually assume a greater investigative and operational role

Interpol has recognised the need for law enforcement officials to acquire specialised knowledge and has developed international training courses and manuals providing useful guidance for investigators working on computer-related crime. Interpol's General Secretariat has also supported the formation of regionally organised working groups comprising local experts in computer-related crime who meet periodically to share experiences and develop best practices. Interpol's General Secretariat has also supported the formation of regionally organised working groups comprising local experts in computer-related crime who meet periodically to share experiences and develop best practices

8. **Do you consider that was useful create a new international police to face this issues and name it like Cyberpol for example?**

Yes, that is a good idea

9. **Do you consider that the coordination between the international and national levels is effective? Why?**

Not very much, no.

10. **In your opinion, what are the main challenges and future trends of cyberthreats?**

Getting more and better data about attacks and level of damage

11. **Many authors consider that Cibersecurity in only possible if the system isn´t connected to the network, in other words, there will be no possible defense if the system is connected. Did you agree with this position? Justify.**

There can be no 100% security in networked systems, yes – but we depend on networked computer for many things nowadays. There always needs to be a cost-benefit analysis, and good risk management

12. **What about the prevention of this type of e-criminality? Is it possible prevent a phenomenon in constant evolution and mutation? How you prospect the criminal prevention of this phenomenon?**

I don't think that prevention is possible. We have to learn how to live with the insecurity in a pragmatic way. Normal criminality can also not be totally prevented

13. **Portugal is beginning to take its first steps in a really Cybersecurity Politic. Our rising in this issue starts with the ratifying of International Cybercrime Convention. In order to finish we want to know what would be more wisely for Portugal in this young journey facing Cibersecurity for real. Give us your advise!**

Ratifying the Cybercrime Convention is a very good idea. In addition, you will need strong public-private partnerships between the government and the private sector. You should also invest in education, for example people specializing in cyber-forensics.

Is there anything else you would like to say about the topic that was not covered in these questions?

<u>Opinions / suggestions / advices:</u>

APÊNDICE 11

Resenha sumária NATo e EUA

APÊNDICE 11

RESENHA SUMÁRIA NATO E EUA

NATO

Esta aliança militar intergovernamental de 28 países tem encetado esforços, através do CCDCOE, rumo a uma política global de Cibersegurança[204].

A NATO é a responsável pela introdução do termo Ciberdefesa na Política de Ciberdefesa adotada em 2008 (Tikk *et all* 2010, 102). Os seus primordiais esforços datam de 1999, quando, durante a Cimeira da NATO em Washington, foram aprovadas as pioneiras iniciativas relacionadas com a segurança das TIC. Em 2002, na Cimeira de Praga, a segurança das informações foi a ordem dos debates do dia. A NATO apoiou a Estónia nos acontecimentos de 2007, e criou um Grupo de trabalho para desenvolver uma política de Ciberdefesa aprovada posteriormente em 2008. Ainda nesta data foram criados o CCDCOE e a NCDMA (Autoridade de Gestão de Ciberdefesa da NATO).

A CCDCOE assume maior relevância dado que a sua missão é promover a cooperação nestes domínios, designadamente: estudos, pesquisas, doutrina, partilha de informações, etc. entre os demais parceiros da aliança bem com terceiros. De salientar ainda que o conceito estratégico de defesa e segurança dos membros da NATO adotado em Lisboa consigna os Ciberataques como sendo "cada vez mais frequente, mais organizados e mais custosos nos danos que infligem nas administrações, negócios e economias dos Estados (…) podendo os mesmos chegar ao limite de ameaçar a segurança prosperidade e estabilidade nacional e do espaço Euro-Atlântico" pelo que se torna necessário "desenvolver a nossa capacidade de prevenir, detetar, defender e recuperar dos Ciberataques"[205] (NATO 2010, 4-5).

[204] Durante a última década a NATO tem feito um esforço significante e mais concretamente orientado para melhorar a sua capacidade militar de Cibersegurança, daí o termo Ciberdefesa.

[205] Tradução nossa.

EUA

Consideramos os EUA como (também sendo) uma grande potência de Cibersegurança[206] pelo que decidimos aqui fazer a justa e breve referência.

Desde cedo, em 1997, "a vulnerabilidade dos sistemas de controlo de voos controlados por computadores foi demostrada com um ataque de *Hackers* contra o aeroporto de Worcester nos EUA"[207] (ITU 2009b, 57). A realidade atual[105] coloca a Cibersegurança no topo das prioridades dos EUA. Desta feita, a NSS apresenta o Cibercrime como uma das principais prioridades de segurança nacional onde o aprimoramento da segurança prevalece e o uso da força está previsto relativamente a este tipo de ameaças (USA 2010, *passim*). "As ameaças à Cibersegurança representam um dos mais sérios desafios de segurança nacional, segurança pública e económicos que enfrentamos enquanto nação"[208] (*ibid.*, 26). Este documento salienta ainda a necessidade de fortalecer parcerias sob o argumento de que "nem o governo, nem o setor privado, nem o cidadão individual pode enfrentar este desafio sozinho"[209] (*ibid.*, 28) fazendo a devida referência a parcerias domésticas e internacionais caraterizadas como urgentes e necessárias. Os EUA assinaram a CC à data da Convenção, sendo a mesma ratificada cinco anos mais tarde transpondo-se para a orla legislativa deste país em 1 de janeiro de 2007.

[206] Salientamos o facto de os EUA serem uma grande potência mitigada fatigantemente por Ciberataques, Touré apresenta os EUA no 1º lugar do *ranking* de Ciberataques, quer como país de destino quer como país de origem desses mesmos ataques (2011, 4-5).
[207] Tradução nossa.
[208] Tradução nossa.
[209] Tradução nossa.

Lisboa, 26 de abril de 2012

N é l s o n T i a g o C a r v a l h o S i l v a
Aspirante a Oficial de Polícia